Remote Management-Referenz

Novell®

ZENworks® 10 Configuration Management SP3

10.3

30. März 2010

www.novell.com

Rechtliche Hinweise

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
USA.
www.novell.com

Online-Dokumentation: Die neueste Online-Dokumentation für dieses und andere Novell-Produkte finden Sie auf der Dokumentations-Webseite (http://www.novell.com/documentation) von Novell.

Novell-Marken

Hinweise zu Novell-Marken finden Sie in der Novell Trademark and Service Mark-Liste (http://www.novell.com/company/legal/trademarks/tmlist.html).

Materialien von Drittanbietern

Die Rechte für alle Marken von Drittanbietern liegen bei den jeweiligen Eigentümern.

Inhalt

Informationen zu diesem Handbuch

In dieser *Fernverwaltungsreferenz für Novell ZENworks 10 Configuration Management* finden Sie Informationen zur Fernverwaltung. Die Informationen in diesem Handbuch gliedern sich wie folgt:

Zielgruppe

Dieses Handbuch richtet sich an Novell® ZENworks®-Administratoren.

Rückmeldungen

Wir freuen uns über Ihre Hinweise, Anregungen und Vorschläge zu diesem Handbuch und den anderen Teilen der Dokumentation zu diesem Produkt. Sie können uns über die Funktion „Kommentare von Benutzern“ im unteren Bereich jeder Seite der Online-Dokumentation oder auf der Website für Feedback zur Novell-Dokumentation (http://www.novell.com/documentation/feedback.html) Ihre Meinung mitteilen.

Zusätzliche Dokumentation

Im Lieferumfang von ZENworks Linux Management finden Sie weitere Dokumentationen (im PDF- und HTML-Format), die Informationen zum Produkt und zu dessen Implementierung beinhalten. Weiteres Dokumentationsmaterial finden Sie in der Dokumentation für ZENworks 10 Configuration Management SP3 (http://www.novell.com/documentation/zcm10/).

Konventionen in der Dokumentation

In dieser Novell-Dokumentation wird ein „Größer als“-Zeichen (>) verwendet, um verschiedene Aktionen innerhalb eines Schritts und Elemente in einem Querverweispfad voneinander zu trennen.

Ein Markensymbol (®, ™ usw.) kennzeichnet eine Novell-Marke. Ein Sternchen (*) kennzeichnet eine Drittanbieter-Marke.

Wenn ein Pfadname für bestimmte Plattformen mit einem umgekehrten Schrägstrich und für andere Plattformen mit einem Schrägstrich geschrieben werden kann, wird der Pfadname in diesem Handbuch mit einem umgekehrten Schrägstrich dargestellt. Benutzer von Plattformen wie Linux*, die einen Schrägstrich erfordern, sollten wie von der Software gefordert Schrägstriche verwenden.

Überblick

1

Mit Novell® ZENworks® Configuration Management können Sie die Fernverwaltung von Geräten über die Verwaltungskonsole vornehmen. Die Fernverwaltung bietet folgende Möglichkeiten:

- Das verwaltete Gerät per Fernzugriff verwalten.
- Die Fernausführung ausführbarer Dateien auf dem verwalteten Gerät vornehmen.
- Dateien zwischen der Verwaltungskonsole und dem verwalteten Gerät übertragen.
- Probleme auf dem verwalteten Gerät diagnostizieren.
- Ein ausgeschaltetes verwaltetes Gerät per Fernzugriff reaktivieren.

Lesen Sie hierzu die folgenden Abschnitte:

- Abschnitt 1.1, „Terminologie der Fernverwaltung“, auf Seite 11
- Abschnitt 1.2, „Zum Verständnis von Fernverwaltungsvorgängen“, auf Seite 12
- Abschnitt 1.3, „Zum Verständnis der Fernverwaltungsfunktionen“, auf Seite 14
- Abschnitt 1.4, „Funktionen des Fernverwaltungs-Proxys“, auf Seite 16

1.1 Terminologie der Fernverwaltung

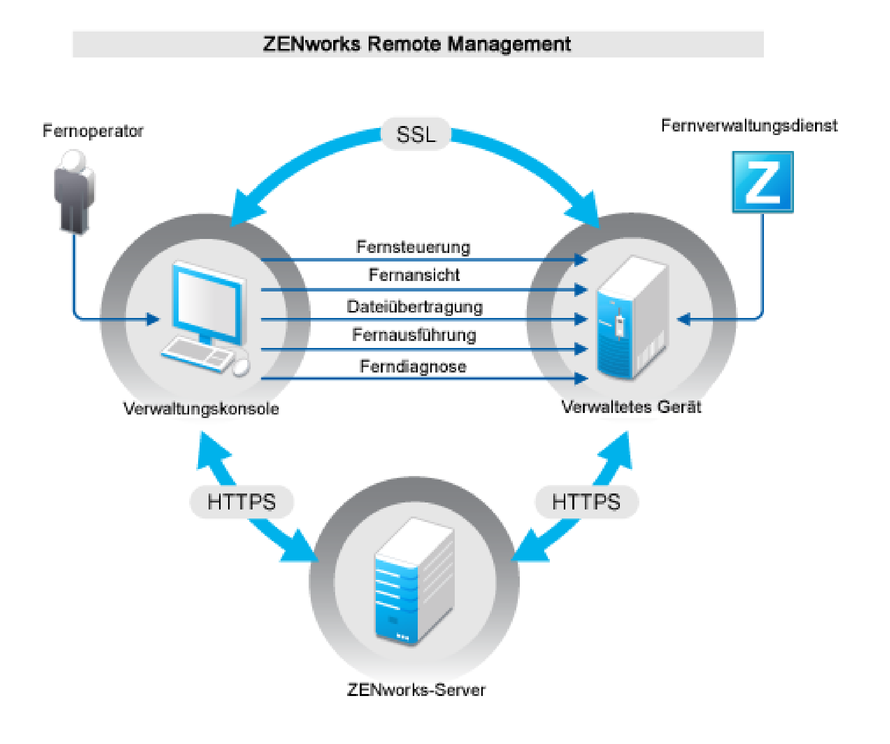
Begriff	Beschreibung
Verwaltetes Gerät	Ein Gerät, das Sie per Fernzugriff verwalten möchten. Zum Verwalten eines Geräts per Fernzugriff müssen Sie sicherstellen, dass die Fernverwaltungskomponente installiert ist und der Fernverwaltungsdienst auf dem Gerät ausgeführt wird.
Verwaltungsserver	Ein Gerät, auf dem der ZENworks Configuration Management-Server installiert ist.
Verwaltungskonsole	Die Schnittstelle für Verwaltung und Administration der Geräte. Zur Ausführung von Fernvorgängen müssen Sie den Fernverwaltungs-Viewer auf der Konsole installieren.
Administrator	Eine Person, die Fernverwaltungsrichtlinien und -einstellungen konfigurieren sowie Fernoperatoren Fernverwaltungsrechte gewähren kann.
Fernverwaltungsdienst	Eine Komponente eines verwalteten Geräts, mit deren Hilfe Fernoperatoren Fernvorgänge auf dem Gerät durchführen können.
Fernverwaltungsvorschau	Eine Verwaltungskonsolenanwendung, mit der ein Fernoperator Fernvorgänge auf dem verwalteten Gerät durchführen kann. Sie ermöglicht es dem Fernoperator, den Desktop des verwalteten Geräts anzuzeigen, Dateien zu übertragen und Anwendungen auf dem verwalteten Gerät auszuführen.
Fernverwaltungs-Listener	Eine Verwaltungskonsolenanwendung, die es einem Fernoperator ermöglicht, Anfragen hinsichtlich der Fernunterstützung von Benutzern an verwalteten Geräten entgegenzunehmen.

Begriff	Beschreibung
Fernverwaltungs-Proxy	Ein Proxyserver, der Fernverwaltungs-Vorgangsanforderungen aus dem Fernverwaltungs-Viewer an ein verwaltetes Gerät weiterleitet. Der Proxy ist nützlich, wenn der Viewer nicht direkt auf ein verwaltetes Gerät zugreifen kann. Dies ist der Fall, wenn sich das Gerät in einem privaten Netzwerk befindet oder auf der anderen Seite einer Firewall oder eines Routers, die/der NAT (Network Address Translation) verwendet. Voraussetzung ist, dass der Proxy auf einem verwalteten Windows-Gerät oder auf einem Linux-Gerät (Primärserver oder Satellitengerät) installiert ist.

1.2 Zum Verständnis von Fernverwaltungsvorgängen

Die Fernverwaltung ermöglicht Administratoren die Steuerung eines Geräts, ohne sich dafür vor Ort begeben zu müssen. Sie hilft Ihnen und Ihrem Unternehmen dabei, Zeit und Geld zu sparen. So können beispielsweise Sie oder der Helpdesk Ihrer Organisation Probleme von verwalteten Geräten per Fernzugriff analysieren und beheben, ohne die Arbeitsstation von Benutzern aufsuchen zu müssen, wodurch der Aufwand für die Problembehandlung reduziert und die Produktivität erhöht wird.

Abbildung 1-1 *Fernverwaltungsoperationen*



In den folgenden Abschnitten werden die unterschiedlichen Vorgänge der Fernverwaltung erläutert:

- Abschnitt 1.2.1, „Fernsteuerung“, auf Seite 13
- Abschnitt 1.2.2, „Fernansicht“, auf Seite 13
- Abschnitt 1.2.3, „Fernausführung“, auf Seite 13
- Abschnitt 1.2.4, „Ferndiagnose“, auf Seite 13
- Abschnitt 1.2.5, „Dateiübertragung“, auf Seite 14
- Abschnitt 1.2.6, „Fernreaktivierung“, auf Seite 14

1.2.1 Fernsteuerung

Mit der Funktion für die Fernsteuerung können Sie das verwaltete Gerät von der Verwaltungskonsole aus fernsteuern und Benutzer bei der Lösung von Geräteproblemen unterstützen.

Die Fernsteuerung stellt eine Verbindung zwischen der Verwaltungskonsole und dem verwalteten Gerät her. Dank Fernsteuerungsverbindungen können Sie alle Vorgänge ausführen, die auch ein Benutzer auf dem Gerät ausführen kann. Weitere Informationen finden Sie unter Abschnitt 3.1, „Verwalten einer Fernsteuerungssitzung“, auf Seite 53.

1.2.2 Fernansicht

Mit der Funktion für die Fernansicht können Sie eine Fernverbindung zu einem verwalteten Gerät herstellen, sodass Sie das verwaltete Gerät anzeigen können, anstatt es zu steuern. Auf diese Weise können Sie Benutzern bei der Lösung auftretender Probleme behilflich sein. Beispielsweise können Sie überprüfen, wie der Benutzer an einem verwalteten Gerät bestimmte Aufgaben erledigt, um sicherzustellen, dass eine Aufgabe korrekt ausgeführt wird. Weitere Informationen finden Sie unter Abschnitt 3.2, „Verwalten einer Fernansichtssitzung“, auf Seite 58.

1.2.3 Fernausführung

Mit der Funktion für die Fernausführung können Sie von der Verwaltungskonsole aus beliebige ausführbare Dateien mit Systemberechtigung auf einem verwalteten Gerät ausführen. Für die Fernausführung einer Anwendung geben Sie den Namen der ausführbaren Datei im Fenster für die Fernausführung an. Sie können beispielsweise den Befehl `regedit` ausführen, um den Registrierungseditor auf dem verwalteten Gerät zu öffnen. Weitere Informationen finden Sie unter Abschnitt 3.3, „Verwalten einer Fernausführungssitzung“, auf Seite 58.

1.2.4 Ferndiagnose

Mit der Funktion für die Ferndiagnose können Sie auf dem verwalteten Gerät aufgetretene Probleme per Fernzugriff diagnostizieren und analysieren. Dadurch wird die Benutzerproduktivität erhöht, da auf den Desktops ohne Unterbrechung weitergearbeitet werden kann. Weitere Informationen finden Sie unter Abschnitt 3.4, „Verwalten einer Ferndiagnosesitzung“, auf Seite 59.

Diagnosen stellen Echtzeit-Informationen bereit, mit deren Hilfe Sie die auf dem verwalteten Gerät aufgetretenen Probleme diagnostizieren und beheben können. Zu den Standarddiagnoseanwendungen auf dem verwalteten Gerät zählen:

- Systemangaben

- Computerverwaltung
- Services
- Registrierungseditor

1.2.5 Dateiübertragung

Mit der Funktion für die Dateiübertragung können Sie verschiedene Dateivorgänge an der Verwaltungskonsole und auf dem verwalteten Gerät durchführen. Sie haben u. a. folgende Möglichkeiten:

- Dateien zwischen der Verwaltungskonsole und dem verwalteten Gerät kopieren
- Dateien oder Ordner umbenennen
- Dateien oder Ordner löschen
- Ordner erstellen
- Eigenschaften von Dateien und Ordnern anzeigen
- Dateien mit der verknüpften Anwendung auf der Verwaltungskonsole öffnen

Weitere Informationen finden Sie unter Abschnitt 3.5, „Verwalten einer Dateiübertragungssitzung“, auf Seite 60.

Wichtig: Mit dem Programm für die Dateiübertragung können Sie auf die Netzlaufwerke des verwalteten Geräts zugreifen.

1.2.6 Fernreaktivierung

Mit der Fernreaktivierung können Sie einen einzelnen Knoten oder eine Gruppe von deaktivierten Knoten in Ihrem Netzwerk per Fernzugriff reaktivieren (vorausgesetzt, auf der Netzwerkkarte im Knoten ist Wake-on-LAN aktiviert). Weitere Informationen finden Sie unter Abschnitt 3.7, „Reaktivieren eines entfernten Geräts“, auf Seite 64.

1.3 Zum Verständnis der Fernverwaltungsfunktionen

In folgenden Abschnitten werden die unterschiedlichen Funktionen der Fernverwaltung erläutert:

* Abschnitt 1.3.11, „Sitzungszusammenarbeit“, auf Seite 16
* Abschnitt 1.3.12, „Fernverwaltungs-Revision“, auf Seite 16

1.3.1 Optisches Signal

Hiermit können Sie den Benutzer auf dem Desktop des verwalteten Geräts optisch darauf hinweisen, dass das Gerät per Fernzugriff verwaltet wird. Das optische Signal gibt Aufschluss über den Fernoperator und die Sitzungsdetails, etwa die Art der Fernsitzung sowie die Anfangszeit der Sitzung. Der Benutzer kann eine bestimmte Fernsitzung beenden oder das Signal-Dialogfeld schließen, um sämtliche Fernsitzungen zu beenden.

1.3.2 Erkennung unbefugter Benutzer

Durch die Funktion zur Erkennung unbefugter Benutzer wird das Risiko, dass das verwaltete Gerät von einem Hacker angegriffen wird, stark verringert. Wenn es dem Fernoperator nicht gelingt, sich innerhalb der angegebenen Anzahl von Versuchen (die Standardeinstellung ist 5 Versuche) beim verwalteten Gerät anzumelden, wird der Fernverwaltungsdienst blockiert und nimmt erst wieder eine Anforderung für eine Fernsitzung an, nachdem die Blockierung aufgehoben wurde.

1.3.3 Sitzungsverschlüsselung

Fernsitzungen werden mithilfe von Secured Socket Layer (TLSv1-Protokoll) geschützt.

1.3.4 Akustisches Signal

Wenn auf dem verwalteten Gerät eine Fernsitzung aktiv ist, können Sie entsprechend der Konfiguration in der Fernverwaltungsrichtlinie in regelmäßigen Abständen ein akustisches Signal auf dem verwalteten Gerät generieren.

1.3.5 Sperrung von Tastatur und Maus

Hiermit können Sie während einer Fernsitzung die Steuerelemente für Tastatur und Maus sperren, um zu verhindern, dass der Benutzer am verwalteten Gerät die Sitzung unterbricht.

Hinweis: Auf verwalteten Windows Vista-Geräten ist das Sperren von Maus und Tastatur nicht möglich, wenn das Thema Aero aktiviert ist.

1.3.6 Bildschirmaustastung

Hiermit können Sie während einer Fernsitzung die Bildschirmanzeige des verwalteten Geräts deaktivieren, um zu verhindern, dass der Benutzer die Vorgänge sieht, die der Fernoperator im Laufe der Sitzung durchführt. Die Tastatur- und Maussteuerung des verwalteten Geräts wird ebenfalls gesperrt.

Hinweis: Durch die Bildschirmaustastung eines verwalteten Tablet PC-Geräts während einer Fernsitzung reduziert sich die Sitzungsleistung.

1.3.7 Abnormale Beendigung

Hiermit können Sie das verwaltete Gerät sperren bzw. den Benutzer am verwalteten Gerät am Zugriff hindern, wenn eine Fernsitzung abrupt getrennt wird.

1.3.8 Überschreiben des Bildschirmschoners

Hiermit können Sie einen passwortgeschützten Bildschirmschoner während einer Fernsitzung auf dem verwalteten Gerät überschreiben.

Hinweis: Diese Funktion steht auf verwalteten Windows Vista*-, Windows Server 2008- und Windows 7-Geräten nicht zur Verfügung.

1.3.9 Automatische Sitzungsbeendigung

Beendet eine Fernsitzung automatisch, wenn für eine angegebene Dauer keine Aktivität zu verzeichnen war.

1.3.10 Vom Agenten gestartete Verbindungen

Hiermit ermöglichen Sie es dem Benutzer am verwalteten Gerät, einen Fernoperator um Unterstützung zu bitten. Sie können die Liste der Fernoperatoren, mit denen der Benutzer Kontakt aufnehmen kann, vorkonfigurieren. Weitere Informationen finden Sie unter Abschnitt 2.8.2, „Initiieren einer Sitzung über das verwaltete Gerät“, auf Seite 44.

Hinweis: Diese Funktion wird zurzeit nur unter Windows unterstützt.

1.3.11 Sitzungszusammenarbeit

Ermöglicht es einer Gruppe von Fernoperatoren, gemeinsam eine Fernsitzung durchzuführen. Der Hauptoperator kann andere Fernoperatoren zur Teilnahme an der Sitzung einladen, zur Behebung eines Problems die Fernsteuerung an einen anderen Fernoperator übergeben, die Steuerung wieder vom Fernoperator zurückfordern und eine Fernsitzung beenden. Weitere Informationen finden Sie unter Abschnitt 3.1.2, „Sitzungszusammenarbeit“, auf Seite 55.

1.3.12 Fernverwaltungs-Revision

Hiermit können Sie für jede auf dem verwalteten Gerät durchgeführte Fernsitzung Revisionsdatensätze generieren. Das Revisionsprotokoll wird auf dem verwalteten Gerät verwaltet und kann vom Benutzer angezeigt werden.

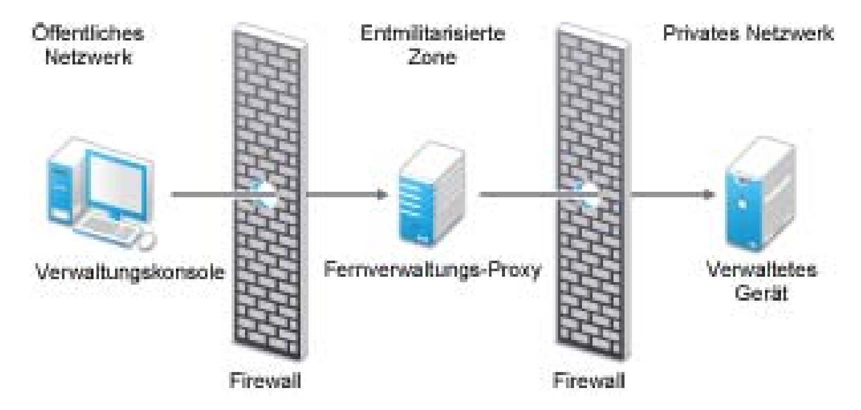
1.4 Funktionen des Fernverwaltungs-Proxys

Auf einem verwalteten Gerät, das sich in einem privaten Netzwerk befindet oder auf der anderen Seite einer Firewall oder eines Routers, die/der NAT (Network Address Translation) verwendet, können Sie keine Fernverwaltungsvorgänge durchführen. Grund hierfür ist, dass die NAT-Firewall die IP-Adresse des Geräts im externen Netzwerk ausblendet und dadurch alle Verbindungsanforderungen an das Gerät sperrt. Für die Fernverwaltung eines solchen Geräts muss der Fernvorgang über einen Fernverwaltungs-Proxy geleitet werden.

Weitere Informationen zur Weiterleitung des Fernvorgangs über einen Proxy nach der Initiierung einer Fernsitzung von der Verwaltungskonsole finden Sie im Abschnitt Durch Proxy weiterleiten im Abschnitt „Installieren einer Fernverwaltungssitzung über den Gerätekontext“ auf Seite 37.

Weitere Informationen zur Weiterleitung des Fernvorgangs über einen Proxy nach der Initiierung einer Fernsitzung aus dem Gerätekontext finden Sie im Abschnitt Durch Proxy weiterleiten im Abschnitt „Initiieren einer Fernverwaltungssitzung über den Benutzerkontext“ auf Seite 40.

Abbildung 1-2 *Fernverwaltungs-Proxy*



Der Proxy muss auf einem Gerät in einer demilitarisierten Zone (DMZ) installiert werden. Das Gerät, auf dem Sie den Proxy installieren, sollte über das öffentliche Netzwerk, in dem sich die Verwaltungskonsole befindet, zugänglich sein und es sollte auf Geräte in einem privaten Netzwerk zugreifen können. Informationen zur Installation des Fernverwaltungs-Proxys erhalten Sie unter Abschnitt 2.10, „Installieren eines Fernverwaltungs-Proxys“, auf Seite 50.

Der Fernverwaltungs-Proxy empfängt eingehende Fernverwaltungsanforderungen vom Fernverwaltungs-Viewer standardmäßig an Port 5750 und leitet die Anforderungen an das Gerät weiter.

Einrichten der Fernverwaltung

2

Die folgenden Abschnitte enthalten Informationen über die Bereitstellung der Fernverwaltungskomponente von Novell® ZENworks® 10 Configuration Management in einer Produktionsumgebung:

2.1 Konfigurieren der Fernverwaltungseinstellungen

Die Fernverwaltungseinstellungen stellen Regeln dar, die das Verhalten oder die Ausführung des Fernverwaltungsdiensts auf dem verwalteten Gerät bestimmen. Die Einstellungen decken die Konfiguration von Ports, Sitzungseinstellungen und Leistungseinstellungen während der Fernsitzung ab. Diese Einstellungen können auf Zonen-, Ordner- und Geräteebene angewendet werden.

Folgende Abschnitte enthalten Informationen zur Konfiguration der Fernverwaltungseinstellungen auf den verschiedenen Ebenen:

2.1.1 Konfigurieren der Fernverwaltungseinstellungen auf der Zonenebene

Standardmäßig gelten die auf Zonenebene konfigurierten Fernverwaltungseinstellungen für alle verwalteten Geräte.

1 Klicken Sie im ZENworks-Kontrollzentrum auf *Konfiguration*.

2 Klicken Sie im Bereich „Verwaltungszoneneinstellungen“ zunächst auf *Geräteverwaltung* und dann auf *Fernverwaltung*.

3 Wählen Sie die Option *Fernverwaltungsdienst ausführen an Port* und geben Sie den Port an, an dem die Ausführung des Fernverwaltungsdiensts aktiviert werden soll.

Standardmäßig überwacht der Fernverwaltungsdienst Port 5950.

4 Wählen Sie die Sitzungseinstellungen aus:

Feld	Details
DNS-Name des Viewers zu Beginn der Fernsitzung ermitteln	Legt fest, dass der Fernverwaltungsdienst den DNS-Namen der Verwaltungskonsole zu Beginn der Fernsitzung ermittelt. Der Name wird in den Revisionsprotokollen gespeichert und während der Fernsitzungen als Teil der Sitzungsinformationen angezeigt. Wenn diese Option nicht aktiviert wird oder der Fernverwaltungsdienst den Konsolennamen nicht finden kann, wird als Konsolenname *unbekannt* angezeigt. Falls im Netzwerk die umgekehrte DNS-Ermittlung nicht aktiviert ist, ist es empfehlenswert, diese Einstellung zu deaktivieren, um beim Starten der Fernsitzung eine erhebliche Verzögerung zu vermeiden.
Fernsitzung zulassen, wenn kein Benutzer am verwalteten Gerät angemeldet ist	Ermöglicht einem Fernoperator die Verwaltung eines Geräts, wenn die Richtlinie den Fernbetrieb zulässt, aber kein Benutzer beim Gerät angemeldet ist. Diese Option ist standardmäßig aktiviert.

5 Treffen Sie unter folgenden Optionen eine Auswahl, um die Leistung einer Fernsitzung zu optimieren:

Feld	Details
Hintergrundbild unterdrücken	Unterdrückt während einer Fernsitzung das Hintergrundbild des verwalteten Geräts. Damit wird verhindert, dass die Bitmap-Daten des Hintergrundbilds wiederholt an die Fernverwaltungskonsole gesendet werden. Auf diese Weise wird eine Leistungsoptimierung der Fernsitzung erzielt.
Optimierungstreiber aktivieren	Aktiviert den Optimierungstreiber, der standardmäßig auf jedem verwalteten Gerät installiert ist. Wenn Sie diese Option auswählen, wird im Rahmen der Fernsitzung lediglich der geänderte Teil des Bildschirms des verwalteten Geräts in der Fernverwaltungskonsole erfasst und aktualisiert. Hierdurch wird eine Leistungsoptimierung der Fernsitzung erzielt.

6 (Optional) Konfigurieren Sie einen Fernverwaltungs-Proxy, um Fernvorgänge auf dem verwalteten Gerät durchzuführen.

Wenn sich das verwaltete Gerät in einem privaten Netzwerk oder auf der anderen Seite einer Firewall oder eines Routers befindet, die/der NAT (Network Address Translation) verwendet, kann der Fernverwaltungsvorgang des Geräts durch einen Fernverwaltungs-Proxy geleitet werden. Sie müssen den Proxy separat installieren. Informationen zur Installation des Fernverwaltungs-Proxys erhalten Sie unter Abschnitt 2.10, „Installieren eines Fernverwaltungs-Proxys“, auf Seite 50.

Aufgabe	Details
Fernverwaltungs-Proxy hinzufügen	1. Klicken Sie auf *Hinzufügen*, um das Dialogfeld „Proxyserver hinzufügen“ anzuzeigen. 2. Füllen Sie die folgenden Felder aus: **Proxy:** Geben Sie die IP-Adresse oder den DNS-Namen der Fernverwaltungskonsole an. **IP-Adressbereich:** Geben Sie die IP-Adressen der Geräte an, deren Fernverwaltung durch den Fernverwaltungs-Proxy erfolgen soll. Sie können den IP-Adressbereich auf eine der folgenden Arten angeben: ◆ Geben Sie den IP-Adressbereich in CIDR-(Classless Inter-Domain Routing-)Notation an. Bei CIDR wird der in Dezimalschreibweise mit Punkten gehaltene Teil der IP-Adresse als Binärzahl mit 32 Bit interpretiert, die in vier Byte mit jeweils 8 Bit aufgeteilt wurde. Die Zahl, die auf den Schrägstrich (/n) folgt, ist die Präfixlänge, also die Anzahl der gemeinsamen Anfangsbits (von der linken Seite der Adresse gezählt). Die /n-Zahl kann zwischen 0 und 32 liegen; 8, 16, 24 und 32 sind hierbei die im Allgemeinen verwendeten Zahlen. Beispiele: 123.45.678.12/16: Gibt alle IP-Adressen an, die mit 123.45 beginnen. 123.45.678.12/24: Gibt alle IP-Adressen an, die mit 123.45.678 beginnen. ◆ Geben Sie den IP-Adressbereich im Format **Von IP-Adresse** - **Bis IP-Adresse** an. Beispiele: 123.45.678.12 - 123.45.678.15: Gibt alle IP-Adressen im Bereich 123.45.678.12 bis 123.45.678.15 an.
Fernverwaltungs-Proxy löschen	1. Wählen Sie den zu löschenden Proxy aus. 2. Klicken Sie auf „Löschen“ und dann auf *OK*.

7 (Optional) Konfigurieren Sie eine Anwendung so, dass sie während der Ferndiagnosesitzung auf dem verwalteten Gerät aufgerufen wird. Hierzu müssen Sie sie der Liste *Diagnoseanwendungen* hinzufügen. Standardmäßig enthält die Liste folgende Anwendungen:

- Systemangaben
- Computerverwaltung
- Services
- Registrierungseditor

In der folgenden Tabelle sind die Aufgaben aufgeführt, die Sie zum Anpassen der Liste *Diagnoseanwendungen* ausführen können:

Job	Details
Anwendung hinzufügen	1. Klicken Sie auf *Hinzufügen.* 2. Geben Sie den Anwendungsnamen und den Anwendungspfad auf dem verwalteten Gerät an. 3. Klicken Sie auf *OK.*
Anwendung löschen	1. Wählen Sie die zu löschende Anwendung aus. 2. Klicken Sie auf „Löschen“ und dann auf *OK*.
Auf Standardanwendungen zurücksetzen	1. Klicken Sie auf *Zurückstellen* und dann auf *OK*.

8 Klicken Sie auf *Übernehmen* und dann auf *OK*.

Diese Änderungen werden nach der Aktualisierung des Geräts auf dem Gerät wirksam.

2.1.2 Konfigurieren der Fernverwaltungseinstellungen auf der Ordnerebene

Standardmäßig werden die auf Zonenebene konfigurierten Fernverwaltungseinstellungen auf alle verwalteten Geräte übertragen. Sie können diese Einstellungen jedoch für die Geräte innerhalb eines Ordners ändern:

1 Klicken Sie im ZENworks-Kontrollzentrum auf *Geräte*.

2 Klicken Sie auf den Ordner (Details), für den Sie die Fernverwaltungseinstellungen konfigurieren möchten.

3 Klicken Sie auf *Einstellungen* und dann auf *Geräteverwaltung* > *Fernverwaltung*.

4 Klicken Sie auf *Einstellungen überschreiben*.

5 Bearbeiten Sie die Fernverwaltungseinstellungen nach Bedarf.

6 Klicken Sie auf *Anwenden*, um die Änderungen zu übernehmen.

oder

Um zu den auf Zonenebene konfigurierten Systemeinstellungen zurückzukehren, klicken Sie auf *Zurückstellen*.

7 Klicken Sie auf *OK*.

Diese Änderungen werden nach der Aktualisierung des Geräts auf dem Gerät wirksam.

2.1.3 Konfigurieren der Fernverwaltungseinstellungen auf der Geräte-Ebene

Standardmäßig werden die auf Zonenebene konfigurierten Fernverwaltungseinstellungen auf alle verwalteten Geräte übertragen. Sie können diese Einstellungen jedoch für das verwaltete Gerät ändern:

1 Klicken Sie im ZENworks-Kontrollzentrum auf *Geräte*.

2 Klicken Sie auf *Server* bzw. *Arbeitsstationen*, um die Liste der verwalteten Geräte anzuzeigen.

3. Klicken Sie auf das Gerät, für das Sie die Fernverwaltungseinstellungen konfigurieren möchten.
4. Klicken Sie auf *Einstellungen* und dann auf *Geräteverwaltung* > *Fernverwaltung*.
5. Klicken Sie auf *Einstellungen überschreiben*.
6. Bearbeiten Sie die Fernverwaltungseinstellungen nach Bedarf.
7. Klicken Sie auf *Anwenden*, um die Änderungen zu übernehmen.

   oder

   Klicken Sie zum Zurücksetzen der zuvor konfigurierten Systemeinstellungen auf dem Gerät auf *Zurückstellen*.

   Falls die Fernverwaltungseinstellungen auf dem Gerät auf Ordnerebene konfiguriert wurden, werden die Einstellungen auf die konfigurierten Einstellungen auf Ordnerebene zurückgestellt. Anderenfalls werden sie auf die Standardeinstellungen auf Zonenebene zurückgestellt.
8. Klicken Sie auf *OK*.

Diese Änderungen werden nach der Aktualisierung des Geräts auf dem Gerät wirksam.

2.2 Aktivieren des Fernverwaltungs-Listeners

So aktivieren Sie einen Fernverwaltungs-Listener zur Überwachung auf Verbindungen von einem verwalteten Gerät:

1. Klicken Sie im ZENworks-Kontrollzentrum auf *Geräte*.
2. Klicken Sie unter *Geräteaufgaben* im linken Fensterbereich auf die Option *Fernverwaltungs-Listener*.
3. Geben Sie im Dialogfeld „Fernverwaltungs-Listener“ den Port an, der auf Fernverbindungen überwacht werden soll. Standardmäßig lautet die Portnummer 5550.
4. Klicken Sie auf *OK*.

   Das Symbol für den ZENworks-Fernverwaltungs-Listener wird im Benachrichtigungsbereich angezeigt.

2.3 Erstellen der Fernverwaltungsrichtlinie

Mit der Fernverwaltungsrichtlinie können Sie das Verhalten bzw. die Ausführung von Fernverwaltungssitzungen auf dem verwalteten Gerät konfigurieren. Die Richtlinie schließt Einstellungen für Fernverwaltungsvorgänge wie Fernsteuerung, Fernansicht, Fernausführung, Ferndiagnose und Dateiübertragung sowie Sicherheitseinstellungen ein.

Standardmäßig wird auf dem verwalteten Gerät eine sichere Fernverwaltungsrichtlinie erstellt, wenn ZENworks Adaptive Agent mit der Fernverwaltungskomponente auf dem Gerät bereitgestellt wird. Die Fernverwaltung von Geräten ist über die Standardrichtlinie möglich. Um die Standardrichtlinie außer Kraft zu setzen, können Sie explizit eine Fernverwaltungsrichtlinie für das Gerät erstellen.

1. Klicken Sie im ZENworks-Kontrollzentrum auf den Karteireiter *Richtlinien*.
2. Klicken Sie in der Liste *Richtlinien* auf *Neu* und danach auf *Richtlinie*, um die Seite „Richtlinientyp auswählen“ anzuzeigen.
3. Wählen Sie *Fernverwaltungsrichtlinie*, klicken Sie auf *Weiter*, um die Seite „Details definieren“ anzuzeigen, und füllen Sie dann die Felder aus:

Richtlinienname: Legen Sie einen eindeutigen Namen für die Richtlinie fest. Der Richtlinienname darf nicht mit dem Namen eines anderen im selben Ordner befindlichen Objekts (Gruppe, Ordner usw.) identisch sein.

Ordner: Geben Sie den Namen ein oder navigieren Sie im ZENworks-Kontrollzentrum zu dem Ordner, in dem die Richtlinie abgelegt werden soll. Der Standardordner ist `/Richtlinien`, Sie können jedoch auch andere Ordner erstellen, um Ihre Richtlinien zu organisieren.

Beschreibung: Geben Sie eine kurze Beschreibung des Inhalts der Richtlinie an. Die Beschreibung wird im ZENworks-Kontrollzentrum auf der Seite „Zusammenfassung" der Richtlinie angezeigt.

4 Klicken Sie auf *Weiter*, um die Seite „Allgemeine Fernverwaltungseinstellungen" anzuzeigen. Wenn Sie die Standardeinstellungen übernehmen möchten, fahren Sie mit dem nächsten Schritt fort. Informationen zur Änderung der Einstellungen finden Sie in folgender Tabelle.

Feld	Details
Benutzern das Anfordern einer Fernsitzung ermöglichen	Ermöglicht es einem Benutzer am verwalteten Gerät, einen Fernoperator zur Durchführung einer Fernsitzung anzufordern. Der Fernoperator muss in diesem Fall sicherstellen, dass der Fernverwaltungs-Listener ausgeführt wird.
Fernsitzung beenden, wenn von einem neuen Benutzer, der sich beim verwalteten Gerät anmeldet, Berechtigungen angefordert werden	Beendet eine laufende Fernsitzung, wenn die Erlaubnis eines neuen Benutzers erforderlich ist, der sich bei einem fernverwalteten Gerät angemeldet hat.
Revisionsinformationen über Fernsitzung für Benutzer am verwalteten Gerät anzeigen	Ermöglicht es einem Benutzer am verwalteten Gerät, die Revisionsdaten zu Fernsitzungen am ZENworks-Symbol zu sehen.
Fernverwaltungseigenschaften über ZENworks-Symbol anzeigen	Ermöglicht es einem Benutzer am verwalteten Gerät, die mit der Fernverwaltungsrichtlinie verbundenen Eigenschaften am ZENworks-Symbol zu sehen.
Bearbeiten	So bearbeiten Sie die Meldung, die für den Benutzer vor Beginn einer Fernsitzung auf dem verwalteten Gerät angezeigt wird: 1. Klicken Sie auf *Bearbeiten*, um das Dialogfeld „Meldung bearbeiten" anzuzeigen. 2. Bearbeiten Sie die Meldung. 3. Klicken Sie auf *OK.*
Standard wiederherstellen	So stellen Sie die Standardmeldung wieder her: 1. Klicken Sie auf *Standard wiederherstellen*, um die Standardmeldung wiederherzustellen.
Fern-Listener hinzufügen	So fügen Sie einen Fern-Listener hinzu: 1. Klicken Sie auf *Hinzufügen*. 2. Geben Sie im Dialogfeld „Fern-Listener hinzufügen" den DNS-Namen oder die IP-Adresse der Verwaltungskonsole sowie die Portnummer ein, den der Fernverwaltungs-Listener auf Fernsitzungsanforderungen überwacht. 3. Klicken Sie auf *OK.*

Feld	Details
Fern-Listener löschen	So löschen Sie einen Fern-Listener: 1. Wählen Sie den zu löschenden Fern-Listener aus. 2. Klicken Sie auf *Löschen*.

5 Klicken Sie auf *Weiter*, um die Seite „Einstellungen für Fernsteuerung" anzuzeigen. Wenn Sie die Standardeinstellungen übernehmen möchten, fahren Sie mit dem nächsten Schritt fort. Informationen zur Änderung der Einstellungen finden Sie in folgender Tabelle.

Feld	Details
Fernsteuerung des verwalteten Geräts zulassen	Ermöglicht Fernsteuerungssitzungen auf dem verwalteten Gerät. Durch Auswahl dieser Option werden die nachfolgenden Optionen auf dieser Seite aktiviert. Wenn diese Option deaktiviert ist, ist für das verwaltete Gerät keine Fernsteuerung möglich.
Vor dem Starten der Fernsteuerung Erlaubnis des Benutzers am verwalteten Gerät einholen	Stellt sicher, dass der Fernoperator den Benutzer am verwalteten Gerät um Erlaubnis bittet, bevor eine Fernsteuerungssitzung gestartet wird.
Während Fernsteuerung optisches Signal an Benutzer am verwalteten Gerät ausgeben	Zeigt während einer Fernsteuerungssitzung ein sichtbares Signal in der oberen rechten Desktopecke des verwalteten Geräts an. Das sichtbare Signal zeigt dem Benutzer am verwalteten Gerät, dass eine Fernsteuerungssitzung aktiv ist.
Akustisches Signal an Benutzer am verwalteten Gerät ausgeben alle [ ] Sekunden während Fernsteuerung	Erzeugt während einer Fernsteuerungssitzung ein akustisches Signal auf dem verwalteten Gerät. Der Signalton wird regelmäßig in dem Sekundenabstand ausgegeben, den der Benutzer festgelegt hat.
Bildschirmaustastung des verwalteten Geräts während Fernsteuerung zulassen	Ermöglicht während einer Fernsteuerungssitzung die Bildschirmaustastung am verwalteten Gerät. Durch Auswahl dieser Option wird außerdem die Tastatur- und Maussteuerung auf dem verwalteten Gerät gesperrt.
Sperren von Maus und Tastatur am verwalteten Gerät während Fernsteuerung zulassen	Ermöglicht während einer Fernsteuerungssitzung das Sperren der Maus und Tastatur am verwalteten Gerät.
Automatisches Entsperren des Bildschirmschoners bei Fernsteuerung zulassen	Ermöglicht vor dem Starten einer Fernsteuerungssitzung auf dem verwalteten Gerät die Aufhebung der Sperre eines passwortgeschützten Bildschirmschoners über den Fernsteuerungs-Viewer.
Fernsteuerungssitzung automatisch beenden nach Inaktivität von [ ] Minuten	Beendet die Fernsteuerungssitzung auf dem verwalteten Gerät, wenn diese für die angegebene Dauer inaktiv ist.

6 Klicken Sie auf *Weiter*, um die Seite „Einstellungen für Fernansicht" anzuzeigen. Wenn Sie die Standardeinstellungen übernehmen möchten, fahren Sie mit dem nächsten Schritt fort. Informationen zur Änderung der Einstellungen finden Sie in folgender Tabelle.

Feld	Details
Fernansicht von verwaltetem Gerät erlauben	Ermöglicht Fernansichtssitzungen am verwalteten Gerät. Durch Auswahl dieser Option werden die nachfolgenden Optionen auf dieser Seite aktiviert. Wenn diese Option deaktiviert ist, ist für das verwaltete Gerät keine Fernansicht möglich.
Vor dem Starten der Fernansicht Erlaubnis des Benutzers am verwalteten Gerät einholen	Stellt sicher, dass der Fernoperator den Benutzer am verwalteten Gerät um Erlaubnis bittet, bevor eine Fernansichtssitzung gestartet wird.
Während Fernansicht optisches Signal an Benutzer am verwalteten Gerät ausgeben	Zeigt während der Fernansichtssitzung ein sichtbares Signal in der oberen rechten Desktopecke des verwalteten Geräts an. Das sichtbare Signal zeigt dem Benutzer am verwalteten Gerät, dass eine Fernansichtssitzung aktiv ist.
Akustisches Signal an Benutzer am verwalteten Gerät ausgeben alle [ ] Sekunden während Fernansicht	Generiert während der Fernansichtssitzung ein akustisches Signal auf dem verwalteten Gerät. Der Signalton wird regelmäßig in dem Sekundenabstand ausgegeben, den der Benutzer festgelegt hat.

7 Klicken Sie auf *Weiter*, um die Seite „Einstellungen für Ferndiagnose“ anzuzeigen. Wenn Sie die Standardeinstellungen übernehmen möchten, fahren Sie mit dem nächsten Schritt fort. Informationen zur Änderung der Einstellungen finden Sie in folgender Tabelle.

Feld	Details
Ferndiagnose des verwalteten Geräts zulassen	Ermöglicht Ferndiagnosesitzungen am verwalteten Gerät. Durch Auswahl dieser Option werden die nachfolgenden Optionen auf dieser Seite aktiviert. Wenn diese Option deaktiviert ist, ist für das verwaltete Gerät keine Ferndiagnose möglich.
Vor dem Starten der Ferndiagnose Erlaubnis des Benutzers am verwalteten Gerät einholen	Stellt sicher, dass der Fernoperator den Benutzer am verwalteten Gerät um Erlaubnis bittet, bevor eine Ferndiagnosesitzung gestartet wird.
Während Ferndiagnose optisches Signal an Benutzer am verwalteten Gerät ausgeben	Zeigt während der Ferndiagnosesitzung ein sichtbares Signal in der oberen rechten Desktopecke des verwalteten Geräts an. Das sichtbare Signal zeigt dem Benutzer am verwalteten Gerät, dass eine Ferndiagnosesitzung aktiv ist.
Akustisches Signal an Benutzer am verwalteten Gerät ausgeben alle [ ] Sekunden während Ferndiagnose	Erzeugt während der Ferndiagnosesitzung ein akustisches Signal auf dem verwalteten Gerät. Der Signalton wird regelmäßig in dem Sekundenabstand ausgegeben, den der Benutzer festgelegt hat.
Bildschirmaustastung des verwalteten Geräts während Ferndiagnose zulassen	Ermöglicht während einer Ferndiagnosesitzung die Bildschirmaustastung am verwalteten Gerät. Tastatur und Maus des verwalteten Geräts sind bei einer Ferndiagnosesitzung stets gesperrt. Durch Auswahl dieser Option wird außerdem das sichtbare Signal am verwalteten Gerät deaktiviert.

Feld	Details
Warnmeldung vor Neustart anzeigen für [ ] Sekunden	Zeigt bei Beginn einer Ferndiagnosesitzung am verwalteten Gerät eine Warnmeldung an, die den Benutzer daran erinnert, den Inhalt aller geöffneten Anwendungen zu speichern. Die Warnmeldung wird für die angegebene Dauer angezeigt, um zu verhindern, dass der Benutzer ungespeicherte Daten verliert, da der Fernoperator während der Ferndiagnosesitzung möglicherweise einen Systemneustart ausführt.
Ferndiagnosesitzung automatisch beenden nach Inaktivität von [ ] Minuten	Beendet die Ferndiagnosesitzung, wenn diese für die angegebene Dauer inaktiv ist.

8 Klicken Sie auf *Weiter*, um die Seite „Einstellungen für Fernausführung“ anzuzeigen. Wenn Sie die Standardeinstellungen übernehmen möchten, fahren Sie mit dem nächsten Schritt fort. Informationen zur Änderung der Einstellungen finden Sie in folgender Tabelle.

Feld	Details
Fernausführung von Programmen an verwaltetem Gerät erlauben	Ermöglicht die Fernausführung von Programmen auf dem verwalteten Gerät. Durch Auswahl dieser Option werden die nachfolgenden Optionen auf dieser Seite aktiviert. Wenn diese Option deaktiviert ist, ist für das verwaltete Gerät keine Fernausführung möglich.
Vor dem Starten der Fernausführung Erlaubnis des Benutzers am verwalteten Gerät einholen	Stellt sicher, dass der Fernoperator den Benutzer am verwalteten Gerät um Erlaubnis bittet, bevor eine Fernausführungssitzung gestartet wird.
Während Fernausführung optisches Signal an Benutzer am verwalteten Gerät ausgeben	Zeigt während der Fernausführungssitzung ein sichtbares Signal in der oberen rechten Desktopecke des verwalteten Geräts an. Das sichtbare Signal zeigt dem Benutzer am verwalteten Gerät, dass eine Fernausführungssitzung aktiv ist.
Ferndiagnosesitzung automatisch beenden nach Inaktivität von [ ] Minuten	Beendet die Fernausführungssitzung, wenn diese für die angegebene Dauer inaktiv ist.

9 Klicken Sie auf *Weiter*, um die Seite „Dateiübertragung“ anzuzeigen. Fahren Sie mit dem nächsten Schritt fort, um die Standardeinstellungen zu akzeptieren, oder ändern Sie die die Standardsicherheitseinstellungen anhand der angegebenen Informationen in der folgenden Tabelle.

Feld	Details
Übertragung von Dateien an verwaltetes Gerät zulassen	Ermöglicht die Übertragung von Dateien zwischen der Verwaltungskonsole und dem verwalteten Gerät. Durch Auswahl dieser Option werden die nachfolgenden Optionen auf dieser Seite aktiviert. Wenn diese Option deaktiviert ist, ist für das verwaltete Gerät keine Dateiübertragung möglich.

Feld	Details
Vor dem Starten der Dateiübertragung Erlaubnis des Benutzers am verwalteten Gerät einholen	Stellt sicher, dass der Fernoperator den Benutzer am verwalteten Gerät um Erlaubnis bittet, bevor eine Dateiübertragungssitzung gestartet wird.
Während Dateiübertragung optisches Signal an Benutzer am verwalteten Gerät ausgeben	Zeigt während der Dateiübertragungssitzung ein sichtbares Signal in der oberen rechten Desktopecke des verwalteten Geräts an. Das sichtbare Signal zeigt dem Benutzer am verwalteten Gerät, dass eine Dateiübertragungssitzung aktiv ist.
Herunterladen von Dateien vom verwalteten Gerät erlauben	Ermöglicht es einem Fernoperator, Dateien auf dem verwalteten Gerät zu öffnen und diese auf die Verwaltungskonsole zu übertragen. Wird diese Option nicht ausgewählt, so kann der Fernoperator nur Dateien von der Verwaltungskonsole auf das verwaltete Gerät übertragen.
Stammverzeichnis bei Dateiübertragung	Geben Sie das Verzeichnis des verwalteten Geräts an, das der Fernoperator während einer Dateiübertragungssitzung sieht. Der Fernoperator kann nur Dateien von und zu diesem Verzeichnis und dessen Unterverzeichnissen übertragen. Das Standardverzeichnis ist „Arbeitsplatz“, was bedeutet, dass der Fernoperator Dateien im gesamten Dateisystem des verwalteten Geräts sehen und übertragen kann.

10 Klicken Sie auf *Weiter*, um das Dialogfeld „Sicherheitseinstellungen“ anzuzeigen. Fahren Sie mit dem nächsten Schritt fort, um die Standardeinstellungen zu akzeptieren, oder ändern Sie die die Standardsicherheitseinstellungen anhand der angegebenen Informationen in der folgenden Tabelle.

Passwortauthentifizierung

Feld	Details
Authentifizierung auf Passwortbasis ermöglichen	Ermöglicht die Authentifizierung des Fernoperators auf dem verwalteten Gerät mittels eines Passworts. Bei Auswahl dieser Option werden die Einstellungen für den Passworttyp aktiviert.
Passwortmindestlänge	Hier legen Sie die Mindestlänge des Passworts fest. Standardmäßig sind 6 Zeichen eingestellt.
Sitzungspasswort	Wählen Sie diese Option aus, um den Benutzer am verwalteten Gerät dazu aufzufordern, vor dem Starten einer neuen Fernsitzung ein Passwort einzugeben. Diese Option wird empfohlen, da das Passwort nicht auf dem verwalteten Gerät gespeichert wird und nur für die aktuelle Sitzung gültig ist.

Feld	Details
Permanentes Passwort	Wählen Sie diese Option aus, um das ZENworks- oder das VNC-Passwort als permanentes Passwort festzulegen. Das ZENworks-Passwort ist sicherer als das VNC-Passwort und wird daher empfohlen. Dieses Passwort kann vom Administrator in der Fernverwaltungsrichtlinie oder vom Benutzer des verwalteten Geräts über das ZENworks-Symbol festgelegt werden. Durch Auswahl dieser Option werden die nachfolgenden Optionen aktiviert. Um es dem Benutzer zu ermöglichen, das Passwort durch Klicken auf das ZENworks-Symbol festzulegen, wählen Sie die Option *Benutzer darf Standardpasswörter auf verwaltetem Gerät überschreiben* aus.
ZENworks-Passwort	So löschen Sie das ZENworks-Passwort: 1. Klicken Sie auf *Passwort löschen*. 2. Klicken Sie auf *Übernehmen* und dann auf *OK*. So legen Sie das ZENworks-Passwort fest: 1. Klicken Sie auf *Passwort festlegen*. 2. Geben Sie das Passwort ein. Die maximale Länge des Passworts beträgt 255 Zeichen. 3. Klicken Sie auf *Übernehmen* und dann auf *OK*.
VNC-Passwort	So löschen Sie das VNC-Passwort: 1. Klicken Sie auf *Passwort löschen*. 2. Klicken Sie auf *Übernehmen* und dann auf *OK*. So legen Sie das VNC-Passwort fest: 1. Klicken Sie auf *Passwort festlegen*. 2. Geben Sie das Passwort ein. Die maximale Länge des Passworts beträgt 8 Zeichen. 3. Klicken Sie auf *Übernehmen* und dann auf *OK*.

Erkennung unbefugter Benutzer

Feld	Details
Erkennung unbefugter Benutzer aktivieren	Wählen Sie diese Option aus, um die Erkennung von ungültigen oder nicht autorisierten Versuchen zum Starten einer Fernsitzung auf dem verwalteten Gerät zu aktivieren. Durch Auswahl dieser Option werden die nachfolgenden Optionen im Abschnitt „Erkennung unbefugter Benutzer“ aktiviert.
Annahme von Verbindungen aussetzen nach [ ] aufeinanderfolgenden ungültigen Versuchen	Geben Sie die maximale Anzahl aufeinanderfolgender ungültiger Versuche an, die ein Fernoperator durchführen darf, bevor der Fernverwaltungsdienst auf dem verwalteten Gerät blockiert wird. Standardmäßig sind es fünf Versuche.

Feld	Details
Annahme von Verbindungen automatisch starten nach [ ] Minuten	Geben Sie die Zeit in Minuten an, nach welcher der Fernverwaltungsagent automatisch eine Verbindung zum verwalteten Gerät versucht. Um die Blockierung des Fernveraltungsservice manuell aufzuheben, doppelklicken Sie auf das ZENworks-Adaptive-Agent-Symbol, klicken Sie auf *Sicherheitseinstellungen* und dann auf *Bei Blockade durch Erkennungsprogramm für unbefugte Benutzer Akzeptieren von Verbindungen aktivieren.* Standardmäßig sind 10 Minuten eingestellt.

Sitzungssicherheit

Feld	Details
Sitzungsverschlüsselung aktivieren	Aktiviert die Verschlüsselung von Sitzungen mithilfe der SSL-Verschlüsselung (TLSv1-Protokoll). Durch Auswahl dieser Option werden die nachfolgenden Optionen im Abschnitt „Sitzungssicherheit" aktiviert.
Verbindung erlauben, wenn Fernverwaltungskonsole über kein SSL-Zertifikat verfügt	Wenn eine Fernverwaltungssitzung vom ZENworks-Kontrollzentrum aus gestartet wird, wird für einen Fernoperator automatisch ein Zertifikat generiert. Dieses Zertifikat wird zur Authentifizierung verwendet. Wählen Sie diese Option, um Verbindungen von einer Fernverwaltungskonsole zu ermöglichen, die außerhalb des ZENworks-Kontrollzentrums gestartet wurde und eventuell nicht über ein SSL-Zertifikat verfügt.
Bis zu [ ] Ebenen in Viewer-Zertifikatkette zulassen	Die auf Rechten und Passwörtern basierenden Novell-Authentifizierungsschemata werden über einen SSL-verschlüsselten Kanal übertragen. Für die Einrichtung dieses Kanals ist es erforderlich, dass der Viewer ein Zertifikat hat. Dieses Zertifikat kann von einer Zwischen- oder Stamm-Zertifizierungsstelle signiert sein und damit eine Zertifikatkette erstellen. Diese Eigenschaft definiert die maximale Anzahl von Ebenen, die in der Zertifikatkette des Anzeigeprogramms zulässig sind. Wenn die ZENworks-interne Zertifizierungsstelle genutzt wird (sie wird standardmäßig installiert), wird automatisch eine zweistufige Viewer-Zertifikatkette angelegt, während eine Fernsitzung vom ZENworks-Kontrollzentrum gestartet wird.

Abnormale Beendigung

Feld	Details
Gerät sperren	Sperrt das verwaltete Gerät, wenn die Fernsitzung nicht ordnungsgemäß beendet wurde.
Benutzer abmelden	Meldet den Benutzer vom verwalteten Gerät ab, wenn die Fernsitzung nicht ordnungsgemäß beendet wurde.

11 Klicken Sie auf *Weiter*, um die Seite „Zusammenfassung“ anzuzeigen.

12 Klicken Sie auf *Fertig stellen*, um die Richtlinie jetzt zu erstellen, oder wählen Sie *Zusätzliche Eigenschaften definieren* aus, um zusätzliche Informationen anzugeben, beispielsweise die Richtlinienzuweisung, die Durchsetzung, den Status und die Gruppe, der die Richtlinie zugehörig ist.

2.4 Konfigurieren von Fernoperatorrechten

Sie können einem Fernoperator Rechte zur Durchführung von Fernsitzungen auf dem verwalteten Gerät zuweisen. Der Fernoperator kann über gerätespezifische und über benutzerspezifische Rechte verfügen.

1 Klicken Sie im ZENworks-Kontrollzentrum auf *Konfiguration.*

2 Klicken Sie in der Kontrollleiste „Administratoren“ auf den Namen des Administrators, dem Fernverwaltungsrechte zugewiesen werden sollen.

3 Klicken Sie in der Kontrollleiste „Zugewiesene Rechte“ auf *Hinzufügen* und dann auf *Fernverwaltungsrechte*, um das Dialogfeld „Fernverwaltungsrechte“ anzuzeigen.

4 Wählen Sie das Gerät oder den Benutzer aus, dem die Rechte erteilt werden sollen.

Die folgende Tabelle enthält Informationen zu den Fernverwaltungsrechten:

Fernverwaltungsrechte	Details
Fernsteuerung	Erteilt dem Fernoperator Rechte zur Fernsteuerung von Geräten.
Fernansicht	Erteilt dem Fernoperator Rechte zur Fernansicht von Geräten.
Ferndiagnose	Erteilt dem Fernoperator Rechte zur Ferndiagnose von Geräten.
Fernausführung	Erteilt dem Fernoperator Rechte zur Fernausführung von Anwendungen auf Geräten.
Dateien übertragen	Weist dem Fernoperator die Rechte zur Übertragung von Dateien an Geräte bzw. von Geräten zu.
Blockierung des Fernverwaltungsdienstes aufheben	Weist dem Fernoperator die Rechte zur Aufhebung der Blockierung des Fernverwaltungsdiensts zu, der aufgrund einer Erkennung unbefugter Benutzer gesperrt wurde.

Hinweis: Die Fernverwaltungsrechte gelten nur für die berechtigungsbasierte Authentifizierung. Der Fernoperator kann einen Fernverwaltungsvorgang jedoch auch über die passwortbasierte Authentifizierung ausführen, sofern die Fernverwaltungsrichtlinie dies zulässt.

5 Klicken Sie auf *OK.*

2.5 Konfigurieren des Fernverwaltungspassworts

Die folgenden Abschnitte enthalten Informationen zur Konfiguration des Fernverwaltungspassworts für den Fernverwaltungsdienst auf dem verwalteten Gerät:

2.5.1 Einrichten des Fernverwaltungspassworts über das ZENworks-Kontrollzentrum

Der Administrator kann während oder nach der Erstellung der Fernverwaltungsrichtlinie auf der Seite „Sicherheitseinstellungen“ ein Fernverwaltungspasswort festlegen.

Informationen darüber, wie Sie beim Erstellen der Fernverwaltungsrichtlinie das Passwort festlegen können, finden Sie unter „Abschnitt 2.3, „Erstellen der Fernverwaltungsrichtlinie“, auf Seite 23“.

So bearbeiten Sie das in der Fernverwaltungsrichtlinie festgelegte Passwort:

1. Klicken Sie im ZENworks-Kontrollzentrum auf *Richtlinien*.
2. Klicken Sie auf die Fernverwaltungsrichtlinie und anschließend auf die Registerkarte *Einstellungen*.
3. Wählen Sie das Passwort im Bereich „Sicherheitseinstellungen“ aus und ersetzen Sie es durch das neue Passwort.
4. Klicken Sie auf *Anwenden*.
5. Erhöhen Sie die Version dieser Richtlinie auf der Seite „Zusammenfassung“ oder unter „Häufige Aufgaben“, um die Änderungen an den Passwörtern auf dem verwalteten Gerät zu aktualisieren.

Gehen Sie wie folgt vor, wenn Sie das Passwort nach der Erstellung der Fernverwaltungsrichtlinie festlegen möchten:

1. Klicken Sie im ZENworks-Kontrollzentrum auf *Richtlinien*.
2. Klicken Sie auf die Fernverwaltungsrichtlinie und anschließend auf die Registerkarte *Einstellungen*.
3. Aktivieren Sie im Bereich „Sicherheitseinstellungen“ die Option *Authentifizierung auf Passwortbasis ermöglichen* und wählen Sie dann die Option *Dauerhaft* aus.
4. Klicken Sie auf *Passwort festlegen* und geben Sie das Passwort an. Wenn Sie das Passwort bereits während der Erstellung der Fernverwaltungsrichtlinie festgelegt haben, können Sie das Passwort bearbeiten. Um das Passwort zu bearbeiten, wählen Sie es aus und ersetzen Sie es durch das neue Passwort.

5. Klicken Sie auf *Anwenden*.
6. Erhöhen Sie die Version dieser Richtlinie auf der Seite „Zusammenfassung“ oder unter „Häufige Aufgaben“, um die Änderungen an den Passwörtern auf dem verwalteten Gerät zu aktualisieren.

2.5.2 Einrichten des Fernverwaltungspassworts über den ZENworks Adaptive Agent

Der Benutzer kann auf dem verwalteten Gerät ein Passwort für den Fernverwaltungsdienst festlegen, wenn die Option *Benutzer darf Standardpasswörter auf verwaltetem Gerät überschreiben* in der Fernverwaltungsrichtlinie aktiviert ist, die auf dem verwalteten Gerät wirksam ist. Dieses Passwort hat Vorrang vor dem Passwort, das in der Fernverwaltungsrichtlinie festgelegt ist.

So legen Sie ein Passwort auf dem verwalteten Gerät fest:

1. Doppelklicken Sie auf das Symbol *ZENworks Adaptive Agent*, um das Fenster für den ZENworks Adaptive Agent anzuzeigen.
2. Wechseln Sie in der linken Kontrollleiste zu *Fernverwaltung* und klicken Sie dann auf *Sicherheit*.
3. Klicken Sie in der rechten Kontrollleiste auf *Passwort festlegen*, um die folgenden Passwörter festzulegen:
   - **ZENworks-Passwort (empfohlen):** Wird für die ZENworks-Authentifizierung verwendet. Sie darf bis zu 255 Zeichen lang sein.
   - **VNC-Passwort:** Wird in VNC-Anwendungen für die Interoperabilität mit Open Source-VNC-Viewern verwendet. Es darf bis zu 8 Zeichen lang sein.
4. Klicken Sie auf *OK*.

2.5.3 Löschen des Fernverwaltungspassworts über das ZENworks-Kontrollzentrum

So löschen Sie das Fernverwaltungspasswort, das über die Richtlinie festgelegt wurde:

1. Klicken Sie im ZENworks-Kontrollzentrum auf *Richtlinien*.
2. Klicken Sie auf die Fernverwaltungsrichtlinie und anschließend auf die Registerkarte *Einstellungen*.
3. Wählen Sie im Bereich „Sicherheitseinstellungen“ die Option *Passwort löschen* aus und klicken Sie dann auf *Anwenden*.
4. Erhöhen Sie die Version dieser Richtlinie auf der Seite „Zusammenfassung“ oder unter „Häufige Aufgaben“, um die Änderungen in der Richtlinie auf dem verwalteten Gerät zu aktualisieren.

So löschen Sie das Fernverwaltungspasswort, das vom Benutzer des verwalteten Geräts festgelegt wurde:

1. Klicken Sie im ZENworks-Kontrollzentrum auf *Richtlinien*.
2. Klicken Sie auf die Fernverwaltungsrichtlinie und anschließend auf die Registerkarte *Einstellungen*.

3. Heben Sie im Bereich „Sicherheitseinstellungen“ die Auswahl der Option *Benutzer darf Standardpasswörter auf verwaltetem Gerät überschreiben* auf und klicken Sie dann auf *Anwenden*.
4. Erhöhen Sie die Version dieser Richtlinie auf der Seite „Zusammenfassung“ oder unter „Häufige Aufgaben“, um die Änderungen in der Richtlinie auf dem verwalteten Gerät zu aktualisieren.

2.5.4 Löschen des Fernverwaltungspassworts über den ZENworks Adaptive Agent

Der Benutzer des verwalteten Geräts kann das von ihm festgelegte Fernverwaltungspasswort zurücksetzen.

1. Doppelklicken Sie auf das Symbol *ZENworks Adaptive Agent*, um das Fenster für den ZENworks Adaptive Agent anzuzeigen.
2. Wechseln Sie in der linken Kontrollleiste zu *Fernverwaltung* und klicken Sie dann auf *Sicherheit*.
3. Klicken Sie in der rechten Kontrollleiste auf *Passwort löschen*, um die Passwörter zu löschen.
4. Klicken Sie auf *OK*.

Das in der Richtlinie konfigurierte Passwort wird wirksam, da kein Passwort vom Benutzer festgelegt wurde.

2.6 Installieren des Fernverwaltungs-Viewers

Der Fernverwaltungs-Viewer ist eine Verwaltungskonsolenanwendung, mit deren Hilfe ein Fernoperator Fernvorgänge auf dem verwalteten Gerät ausführen kann. Sie ermöglicht es dem Fernoperator, den Desktop des verwalteten Geräts anzuzeigen, Dateien zu übertragen und Anwendungen auf dem verwalteten Gerät auszuführen.

Klicken Sie zum Installieren des Fernverwaltungs-Viewers auf den Link *Fernverwaltungs-Viewer installieren*, der im ZENworks-Kontrollzentrum angezeigt wird, wenn Sie einen Fernverwaltungsvorgang am verwalteten Gerät ausführen. Dieser Link wird nur angezeigt, wenn Sie den Fernverwaltungsvorgang auf dem Gerät zum ersten Mal durchführen und wenn der Viewer noch nicht auf dem Gerät installiert ist.

Wenn bereits eine ältere Version des Fernverwaltungs-Viewer auf dem Gerät installiert ist, wird der Link *Fernverwaltungs-Viewer aktualisieren* angezeigt. Klicken Sie auf diesen Link, um die Version des auf dem Gerät installierten Viewers zu aktualisieren.

Hinweis: Für die Installation des Fernverwaltungs-Viewers unter SUSE® Linux Enterprise Server 11 (SLES 11) oder SUSE Linux Enterprise Desktop 11 (SLED 11) ist das entsprechende glitz-Paket erforderlich. Sie müssen das passende glitz-Paket von der openSUSE®-Website (http://software.opensuse.org/112/en) herunterladen und installieren.

Unter Windows:

1. Klicken Sie im ZENworks-Kontrollzentrum auf *Konfiguration*.
2. Klicken Sie im linken Navigationsbereich auf *ZENworks-Tools herunterladen*.
3. Klicken Sie im linken Navigationsbereich der Seite „ZENworks-Download“ auf *Verwaltung*.

4 Klicken Sie auf `novell-zenworks-rm-viewer-<version>.msi`.

5 (Bedingt) Wenn Sie das ZENworks-Kontrollzentrum über Internet Explorer* gestartet haben, führen Sie eine der folgenden Aktionen aus:

- Klicken Sie zur Installation des Viewers auf *Ausführen*.
- Klicken Sie auf *Speichern*, um die Datei an einem temporären Speicherort zu speichern. Doppelklicken Sie auf die Datei, um den Viewer zu installieren.

6 (Bedingt) Wenn Sie das ZENworks-Kontrollzentrum über Firefox gestartet haben, klicken Sie zum Speichern der Datei an einem vorläufigen Speicherort auf *Datei speichern*. Doppelklicken Sie danach auf die Datei, um den Viewer zu installieren.

Unter Linux:

1 Klicken Sie im ZENworks-Kontrollzentrum auf *Konfiguration*.

2 Klicken Sie im linken Navigationsbereich auf *ZENworks-Tools herunterladen*.

3 Klicken Sie im linken Navigationsbereich der Seite „ZENworks-Download“ auf *Verwaltung*.

4 Klicken Sie auf `novell-zenworks-rm-viewer-<version>.noarch.rpm`.

5 Entscheiden Sie, ob der Viewer sofort installiert werden soll oder ob die RPM-Datei für den Viewer zur späteren Installation gespeichert werden soll.

- Klicken Sie zur sofortigen Installation des Viewers auf *Öffnen mit*, um den Fernverwaltungs-Viewer mit zen-installer zu öffnen, geben Sie das Root-Passwort an und klicken Sie anschließend auf *OK*.
- Sie können die Viewer-RPM-Datei auch in das beim Herunterladen vorgeschlagene Standardverzeichnis speichern und den Viewer zu einem späteren Zeitpunkt installieren. Klicken Sie dazu auf *Auf Datenträger speichern*. Führen Sie eine der folgenden Aktionen aus, um die RPM-Datei zu installieren:
  - Klicken Sie auf die RPM-Datei für den Viewer, geben Sie das Root-Passwort an, und klicken Sie anschließend auf *OK*.
  - Führen Sie den folgenden Befehl als Superuser oder Root-Benutzer aus:

    ```
    rpm -ivh novell-zenworks-rm-viewer-<version>.noarch.rpm
    ```

2.7 Aktualisieren des Fernverwaltungs-Viewers

Wenn Sie auf einem von Windows verwalteten Gerät mit einer früheren Version des Fernverwaltungs-Viewers einen Fernverwaltungsvorgang durchführen, wird im ZENworks-Kontrollzentrum der Link *Fernverwaltungs-Viewer aktualisieren* angezeigt. Klicken Sie auf diesen Link, um die Version des auf dem Gerät installierten Viewers zu aktualisieren.

Um den Fernverwaltungs-Viewer auf einem Linux-Gerät von Novell ZENworks 10 Configuration Management SP2 (10.2) auf Novell ZENworks 10 Configuration Management SP3 (10.3) oder höher zu aktualisieren, führen Sie folgenden Befehl als Superbenutzer oder Root-Benutzer aus:

```
rpm -Uvh --nopostun novell-zenworks-rm-viewer-<version>.noarch.rpm
```

Sie können auch die alte Version `novell-zenworks-rm-viewer-10.x.x.rpm` deinstallieren und die neue Version installieren. Weitere Informationen zur Installation des Viewers erhalten Sie unter Abschnitt 2.6, „Installieren des Fernverwaltungs-Viewers“, auf Seite 34.

2.8 Starten von Fernverwaltungsvorgängen

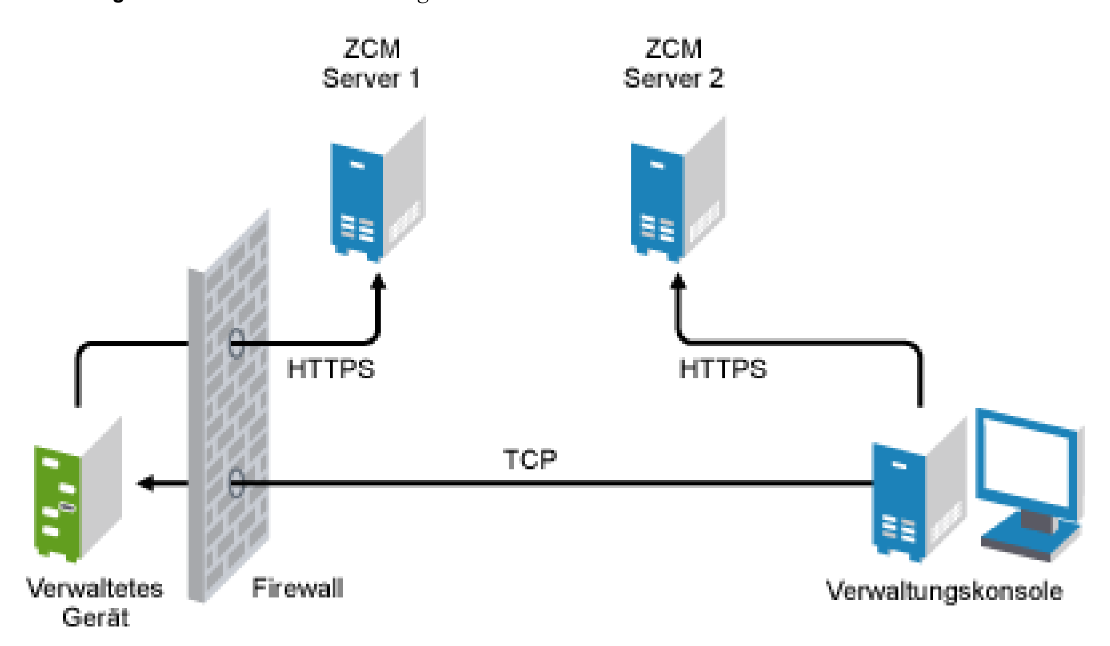
Der Fernvorgang kann auf folgende Weisen initiiert werden:

- Abschnitt 2.8.1, „Initiieren einer Sitzung über die Verwaltungskonsole“, auf Seite 36
- Abschnitt 2.8.2, „Initiieren einer Sitzung über das verwaltete Gerät“, auf Seite 44

2.8.1 Initiieren einer Sitzung über die Verwaltungskonsole

In diesem Szenario wird die Fernsitzung vom Administrator an der Verwaltungskonsole initiiert. Die Verwaltungskonsole befindet sich üblicherweise innerhalb eines Unternehmensnetzwerks; das verwaltete Gerät kann sich entweder innerhalb oder außerhalb des Unternehmensnetzwerks befinden. Folgende Illustration zeigt eine Fernsitzung, die über die Verwaltungskonsole auf dem verwalteten Gerät initiiert wurde.

Abbildung 2-1 *Konsoleninitiierte Sitzung*



Der Fernverwaltungsagent startet automatisch, sobald das verwaltete Gerät gebootet wird. Bei der Bereitstellung des Geräts wird eine Standardrichtlinie für die Fernverwaltung auf dem verwalteten Gerät erstellt. Eine Fernverwaltung des Geräts mit dieser Standardrichtlinie ist nur im rechtebasierten Authentifizierungsmodus möglich. Bei Erstellung einer neuen Fernverwaltungsrichtlinie setzt die neue Richtlinie die Standardrichtlinie außer Kraft.

Wenn sich die ZENworks-Verwaltungszone über zwei oder mehr NAT-fähige private Netzwerke erstreckt, die durch ein öffentliches Netzwerk verbunden sind, müssen Sie auf den Gateways dieser privaten Netzwerke DNS_ALG bereitstellen. DNS_ALG stellt sicher, dass die durch ZENworks-Komponenten initiierten DNS-Lookup-Abfragen den korrekten, der privaten Adresse zugeordneten Hostnamen zurückgeben, und ermöglicht dadurch die Kommunikation zwischen der Verwaltungskonsole und den verwalteten Geräten. Weitere Informationen zu DNS_ALG erhalten Sie im Dokument „DNS ALG RFC - 2694“ (http://www.ietf.org/rfc/rfc2694).

Wenn Sie ein Geräte mithilfe des DNS-Namens fernverwalten möchten, vergewissern Sie sich, dass der Dienst Dynamic DNS im Netzwerk bereitgestellt ist.

Der Fernoperator hat folgende Möglichkeiten, um eine Sitzung einzuleiten:

- „Starten eines Fernverwaltungsvorgangs über das ZENworks-Kontrollzentrum“ auf Seite 37
- „Starten eines Fernverwaltungsvorgangs im Einzelmodus“ auf Seite 43
- „Starten eines Fernverwaltungsvorgangs mithilfe von Befehlszeilenoptionen.“ auf Seite 43

Starten eines Fernverwaltungsvorgangs über das ZENworks-Kontrollzentrum

Die verschiedenen Fernverwaltungsvorgänge können aus dem Gerätekontext oder dem Benutzerkontext eingeleitet werden:

- „Installieren einer Fernverwaltungssitzung über den Gerätekontext“ auf Seite 37
- „Initiieren einer Fernverwaltungssitzung über den Benutzerkontext“ auf Seite 40

Installieren einer Fernverwaltungssitzung über den Gerätekontext

So leiten Sie eine Fernverwaltungssitzung auf einem Gerät ein

1. Klicken Sie im ZENworks-Kontrollzentrum auf den Karteireiter *Geräte*.
2. Klicken Sie auf *Server* oder *Arbeitsstationen* und wählen Sie das Gerät aus, das Sie per Fernzugriff verwalten möchten. Klicken Sie auf *Aktion* und wählen Sie dann den Fernverwaltungsvorgang aus, den Sie ausführen möchten.

   oder

   Wählen Sie unter *Geräteaufgaben* in der linken Kontrollleiste den Fernverwaltungsvorgang aus, den Sie ausführen möchten.

   Folgende Vorgänge sind verfügbar:

   - **Fernsteuerung:** Zeigt das Dialogfeld „Fernverwaltung“ an, über das Sie einen Fernsteuerungs-, Fernansichts- oder Fernausführungsvorgang auf dem verwalteten Gerät ausführen können.
   - **Fenster für die Ferndiagnose:** Zeigt das Dialogfeld „Ferndiagnose“ an, über das Sie einen Ferndiagnosevorgang auf dem verwalteten Gerät ausführen können.
   - **Dateien übertragen:** Zeigt das Dialogfeld „Dateiübertragung“ an, über das Sie einen Dateiübertragungsvorgang auf dem verwalteten Gerät ausführen können.
3. Tragen Sie die Optionen im angezeigten Dialogfeld ein. Die folgende Tabelle enthält Informationen zu den verschiedenen verfügbaren Optionen:

Feld	Details
Gerät	Geben Sie den Hostnamen oder die IP-Adresse des Gerätes an, das Sie per Fernzugriff verwalten möchten.
Vorgang	Wählen Sie den Typ für den Fernvorgang aus, den Sie am verwalteten Gerät durchführen möchten. Diese Option steht nur im Dialogfeld „Fernverwaltung“ zur Verfügung.
Anwendung	Wählen Sie die Anwendung aus, die Sie auf dem Gerät für die Ferndiagnose verwenden möchten. Diese Option steht nur im Dialogfeld „Ferndiagnose“ zur Verfügung.
Authentifizierung	Wählen Sie den gewünschten Modus aus, um sich am verwalteten Gerät zu authentifizieren. Die verschiedenen Authentifizierungsmodi lauten: ◆ Rechtsbasierte Authentifizierung ◆ Passwortbasierte Authentifizierung
Anschluss	Geben Sie die Nummer des Ports an, den der Fernverwaltungsagent überwacht. Standardmäßig lautet die Portnummer 5950
Sitzungsmodus	Wählen Sie einen der folgenden Modi für die Sitzung aus: ◆ **Zusammenarbeit:** Mithilfe dieser Option können Sie eine Fernsteuerungssitzung und eine Fernansichtsitzung im Modus „Zusammenarbeit“ starten. Dieser Modus wird standardmäßig für den Fernsteuerungsvorgang ausgewählt. Wenn Sie zuerst die Fernsteuerungssitzung auf dem verwalteten Gerät starten, erhalten Sie die Privilegien eines Master-Fernoperators. Dazu gehören: ◆ Einladen anderer Fernoperatoren zum Beitritt der Fernsitzung ◆ Delegieren von Fernsteuerungsrechten an einen Fernoperator ◆ Wiedererlangen der Steuerung von einem Fernoperator ◆ Beenden einer Fernsitzung. Die nachfolgenden gestarteten Sitzungen sind Fernansichtssitzungen. **Hinweis:** Der Zusammenarbeitsmodus wird auf Linux noch nicht unterstützt. ◆ **Freigegeben:** Mehreren Fernoperatoren gleichzeitig die Fernsteuerung des verwalteten Geräts ermöglichen. ◆ **Exklusiv:** Ermöglicht Ihnen eine exklusive Fernsteuerungssitzung auf dem verwalteten Gerät. Nachdem eine Sitzung im exklusiven Modus gestartet wurde, kann keine andere Fernsitzung auf dem verwalteten Gerät gestartet werden. Dieser Modus wird standardmäßig für den Fernansichtsvorgang ausgewählt. Diese Option steht nur im Dialogfeld „Fernverwaltung“ zur Verfügung.
Sitzungsver-schlüsselung	Gewährleistet, dass die Fernsitzung mithilfe der SSL-(Secure Sockets Layer-)Verschlüsselung (TLSv1-Protokoll) geschützt wird.
Caching aktivieren	Verbessert die Leistung durch Speichern der Fernverwaltungs-Sitzungsdaten im Cache. Diese Option steht für Fernsteuerungs- und Ferndiagnosevorgänge sowie für Fernansichtsaktionen zur Verfügung. Diese Option wird zurzeit nur unter Windows unterstützt.

Feld	Details
Dynamische Bandbreitenoptimierung	Verbessert die Leistung durch Erkennung der verfügbaren Netzwerkbandbreite und Anpassung der Sitzungseinstellungen an die erkannte Bandbreite. Diese Option steht für Fernsteuerungs- und Ferndiagnosevorgänge sowie für Fernansichtsaktionen zur Verfügung.
Protokollierung aktivieren	Protokolliert Sitzungs- und Debug-Informationen in der Datei `novell-zenworks-vncviewer.txt` Die Datei wird standardmäßig auf dem Desktop gespeichert, wenn Sie das ZENworks-Kontrollzentrum (ZCC) über Internet Explorer starten, oder im installierten Mozilla-Verzeichnis, wenn Sie ZCC über Mozilla * FireFox*starten.
Durch Proxy weiterleiten	Ermöglicht die Weiterleitung des Fernverwaltungsvorgangs des verwalteten Geräts durch einen Fernverwaltungs-Proxy. Wenn sich das verwaltete Gerät in einem privaten Netzwerk oder auf der anderen Seite einer Firewall oder eines Routers befindet, die/der NAT (Network Address Translation) verwendet, kann der Fernverwaltungsvorgang des Geräts durch einen Fernverwaltungs-Proxy geleitet werden. Diese Option wird zurzeit nur unter Windows unterstützt. Füllen Sie die folgenden Felder aus: **Proxy:** Geben Sie den DNS-Namen bzw. die IP-Adresse des Geräts des Fernverwaltungs-Proxys an. Standardmäßig wird der Proxy, der in der Kontrollleiste Proxy-Einstellungen für den Fernvorgang auf dem Gerät konfiguriert wurde, in diesem Feld eingegeben. Sie können einen anderen Proxy angeben. **Proxy-Port:** Geben Sie die Nummer des Ports an, den der Fernverwaltungs-Proxy überwacht. Standardmäßig lautet die Portnummer 5750. **Hinweis:** Die Fernverwaltungs-Revision zeigt die IP-Adresse des Geräts an, das auf dem Fernverwaltungs-Proxy läuft und nicht die IP-Adresse der Verwaltungskonsole.
Das folgende Schlüsselpaar zur Identifizierung verwenden	Wenn eine interne Zertifizierungsstelle (CA) genutzt wird, werden die folgenden Optionen nicht angezeigt. Wenn eine externe Zertifizierungsstelle (CA) genutzt wird, füllen Sie die folgenden Felder aus: **Privater Schlüssel:** Klicken Sie auf *Durchsuchen*, um zum privaten Schlüssel des Fernoperators zu navigieren und diesen auszuwählen. **Zertifikat:** Klicken Sie auf *Durchsuchen*, um zum Zertifikat zu navigieren, das dem privaten Schlüssel entspricht, und dieses auszuwählen. Dieses Zertifikat muss mit der Zertifizierungsstelle verknüpft sein, die für die Zone konfiguriert ist. Die unterstützten Formate für den Schlüssel und das Zertifikat sind DER, PEM und PFX. Wenn das Format PFX benutzt wird, müssen der Schlüssel und das Zertifikat in derselben Datei zur Verfügung stehen. Sie müssen diese Datei als Eingabe sowohl für den Schlüssel als auch für das Zertifikat angeben. **Cache-Pfad aktivieren:** Legt fest, dass die Primärschlüssel- und Zertifikatpfade auf der Verwaltungskonsole zwischengespeichert werden. Diese Option wird zurzeit nur unter Windows unterstützt.

4 Klicken Sie auf *OK*, um den ausgewählten Fernverwaltungsvorgang zu starten.

Initiieren einer Fernverwaltungssitzung über den Benutzerkontext

Wenn Sie einem Benutzer helfen möchten, indem Sie eine Fernsitzung auf dem verwalteten Gerät ausführen, bei dem er sich angemeldet hat:

1. Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte *Benutzer*.
2. Klicken Sie auf die *Benutzerquelle*.
3. Wählen Sie den Benutzer aus, um das Gerät, auf dem er angemeldet ist, per Fernzugriff zu verwalten.
4. Klicken Sie auf *Aktion* und wählen Sie dann den Fernverwaltungsvorgang aus, den Sie ausführen möchten.

   Folgende Vorgänge sind verfügbar:

   - **Fernsteuerung:** Zeigt das Dialogfeld „Fernverwaltung“ an, über das Sie einen Fernsteuerungs-, Fernansichts- oder Fernausführungsvorgang auf dem verwalteten Gerät ausführen können.
   - **Fenster für die Ferndiagnose:** Zeigt das Dialogfeld „Ferndiagnose“ an, über das Sie einen Ferndiagnosevorgang auf dem verwalteten Gerät ausführen können.
   - **Dateien übertragen:** Zeigt das Dialogfeld „Dateiübertragung“ an, über das Sie einen Dateiübertragungsvorgang auf dem verwalteten Gerät ausführen können.
5. Tragen Sie die Optionen im angezeigten Dialogfeld ein. Die folgende Tabelle enthält Informationen zu den verschiedenen verfügbaren Optionen:

Feld	Details
Gerät	Geben Sie den Hostnamen oder die IP-Adresse des Gerätes an, das Sie per Fernzugriff verwalten möchten.
Vorgang	Wählen Sie den Typ für den Fernvorgang aus, den Sie am verwalteten Gerät durchführen möchten. Diese Option steht nur im Dialogfeld „Fernverwaltung“ zur Verfügung.
Anwendung	Wählen Sie die Anwendung aus, die Sie auf dem Gerät für die Ferndiagnose verwenden möchten. Diese Option steht nur im Dialogfeld „Ferndiagnose“ zur Verfügung.
Authentifizierung	Wählen Sie den gewünschten Modus aus, um sich am verwalteten Gerät zu authentifizieren. Die verschiedenen Authentifizierungsmodi lauten: ◆ Rechtsbasierte Authentifizierung ◆ Passwortbasierte Authentifizierung
Anschluss	Geben Sie die Nummer des Ports an, den der Fernverwaltungsagent überwacht. Standardmäßig lautet die Portnummer 5950
Sitzungsmodus	Wählen Sie einen der folgenden Modi für die Sitzung aus: ◆ **Zusammenarbeit:** Mithilfe dieser Option können Sie eine Fernsteuerungssitzung und eine Fernansichtsitzung im Modus „Zusammenarbeit“ starten. Dieser Modus wird standardmäßig für den Fernsteuerungsvorgang ausgewählt. Wenn Sie zuerst die Fernsteuerungssitzung auf dem verwalteten Gerät starten, erhalten Sie die Privilegien eines Master-Fernoperators. Dazu gehören: ◆ Einladen anderer Fernoperatoren zum Beitritt der Fernsitzung ◆ Delegieren von Fernsteuerungsrechten an einen Fernoperator ◆ Wiedererlangen der Steuerung von einem Fernoperator ◆ Beenden einer Fernsitzung. Die nachfolgenden gestarteten Sitzungen sind Fernansichtssitzungen. **Hinweis:** Der Zusammenarbeitsmodus wird auf Linux noch nicht unterstützt. ◆ **Freigegeben:** Mehreren Fernoperatoren gleichzeitig die Fernsteuerung des verwalteten Geräts ermöglichen. ◆ **Exklusiv:** Ermöglicht Ihnen eine exklusive Fernsteuerungssitzung auf dem verwalteten Gerät. Nachdem eine Sitzung im exklusiven Modus gestartet wurde, kann keine andere Fernsitzung auf dem verwalteten Gerät gestartet werden. Dieser Modus wird standardmäßig für den Fernansichtsvorgang ausgewählt. Diese Option steht nur im Dialogfeld „Fernverwaltung“ zur Verfügung.
Sitzungsverschlüsselung	Gewährleistet, dass die Fernsitzung mithilfe der SSL-(Secure Sockets Layer-)Verschlüsselung (TLSv1-Protokoll) geschützt wird.
Caching aktivieren	Verbessert die Leistung durch Speichern der Fernverwaltungs-Sitzungsdaten im Cache. Diese Option steht für Fernsteuerungs- und Ferndiagnosevorgänge sowie für Fernansichtsaktionen zur Verfügung. Diese Option wird zurzeit nur unter Windows unterstützt.

Feld	Details
Dynamische Bandbreitenoptimierung	Verbessert die Leistung durch Erkennung der verfügbaren Netzwerkbandbreite und Anpassung der Sitzungseinstellungen an die erkannte Bandbreite. Diese Option steht für Fernsteuerungs- und Ferndiagnosevorgänge sowie für Fernansichtsaktionen zur Verfügung.
Protokollierung aktivieren	Protokolliert Sitzungs- und Debug-Informationen in der Datei `novell-zenworks-vncviewer.txt` Die Datei wird standardmäßig auf dem Desktop gespeichert, wenn Sie das ZENworks-Kontrollzentrum (ZCC) über Internet Explorer starten, oder im installierten Mozilla-Verzeichnis, wenn Sie ZCC über Mozilla * FireFox*starten.
Durch Proxy weiterleiten	Ermöglicht die Weiterleitung des Fernverwaltungsvorgangs des verwalteten Geräts durch einen Fernverwaltungs-Proxy. Wenn sich das verwaltete Gerät in einem privaten Netzwerk oder auf der anderen Seite einer Firewall oder eines Routers befindet, die/der NAT (Network Address Translation) verwendet, kann der Fernverwaltungsvorgang des Geräts durch einen Fernverwaltungs-Proxy geleitet werden. Diese Option wird zurzeit nur unter Windows unterstützt. Füllen Sie die folgenden Felder aus: **Proxy:** Geben Sie den DNS-Namen bzw. die IP-Adresse des Geräts des Fernverwaltungs-Proxys an. Standardmäßig wird der Proxy, der in der Kontrollleiste Proxy-Einstellungen für den Fernvorgang auf dem Gerät konfiguriert wurde, in diesem Feld eingegeben. Sie können einen anderen Proxy angeben. **Proxy-Port:** Geben Sie die Nummer des Ports an, den der Fernverwaltungs-Proxy überwacht. Standardmäßig lautet die Portnummer 5750. **Hinweis:** Die Fernverwaltungs-Revision zeigt die IP-Adresse des Geräts an, das auf dem Fernverwaltungs-Proxy läuft und nicht die IP-Adresse der Verwaltungskonsole.
Das folgende Schlüsselpaar zur Identifizierung verwenden	Wenn eine interne Zertifizierungsstelle (CA) genutzt wird, werden die folgenden Optionen nicht angezeigt. Wenn eine externe Zertifizierungsstelle (CA) genutzt wird, füllen Sie die folgenden Felder aus: **Privater Schlüssel:** Klicken Sie auf *Durchsuchen*, um zum privaten Schlüssel des Fernoperators zu navigieren und diesen auszuwählen. **Zertifikat:** Klicken Sie auf *Durchsuchen*, um zum Zertifikat zu navigieren, das dem privaten Schlüssel entspricht, und dieses auszuwählen. Dieses Zertifikat muss mit der Zertifizierungsstelle verknüpft sein, die für die Zone konfiguriert ist. Die unterstützten Formate für den Schlüssel und das Zertifikat sind DER, PEM und PFX. Wenn das Format PFX benutzt wird, müssen der Schlüssel und das Zertifikat in derselben Datei zur Verfügung stehen. Sie müssen diese Datei als Eingabe sowohl für den Schlüssel als auch für das Zertifikat angeben. **Cache-Pfad aktivieren:** Legt fest, dass die Primärschlüssel- und Zertifikatpfade auf der Verwaltungskonsole zwischengespeichert werden. Diese Option wird zurzeit nur unter Windows unterstützt.

6 Klicken Sie auf *OK*, um den ausgewählten Fernvorgang zu starten.

Starten eines Fernverwaltungsvorgangs im Einzelmodus

Installieren Sie vor dem Starten des Fernverwaltungsvorgangs im eigenständigen Modus den Fernverwaltungs-Viewer. Informationen zur Installation des Viewers erhalten Sie unter Abschnitt 2.6, „Installieren des Fernverwaltungs-Viewers“, auf Seite 34.

So starten Sie einen Fernverwaltungsvorgang im Einzelmodus:

1. Doppelklicken Sie auf die Datei `nzrViewer.exe`, um den ZENworks-Fernverwaltungs-Client zu starten.
2. Geben Sie im angezeigten Fenster „ZENworks-Fernverwaltungsverbindung“ den DNS-Namen bzw. die IP-Adresse des verwalteten Geräts und die Portnummer im Format *IP-Adresse~~Port* an. Beispiel: 10.0.0.0~~1000.
3. Geben Sie den DNS-Namen oder die IP-Adresse des Fernverwaltungs-Proxys sowie die Portnummer in einem der folgenden Formate an:
   - *IP-Adresse~~Port*. Zum Beispiel 10.0.0.0~~5750.
   - *IP-Adresse~Port*. Zum Beispiel 10.0.0.0~50.
4. Klicken Sie auf *Verbinden*.

   Bei erfolgreicher Authentifizierung wird die Fernsitzung gestartet. Standardmäßig wird eine Fernsteuerungssitzung gestartet.

Starten eines Fernverwaltungsvorgangs mithilfe von Befehlszeilenoptionen.

Wenn Sie über die Befehlszeile Fernverwaltungsvorgänge ausführen möchten, müssen Sie den Fernverwaltungs-Viewer zunächst installieren. Informationen zur Installation des Viewers erhalten Sie unter Abschnitt 2.6, „Installieren des Fernverwaltungs-Viewers“, auf Seite 34.

So starten Sie den Fernverwaltungsvorgang mithilfe der Befehlszeilenoptionen:

1. Wechseln Sie an der Eingabeaufforderung in das Verzeichnis, in dem der Viewer installiert ist. Der Viewer ist standardmäßig im Verzeichnis `<Ordner_mit_Benutzeranwendungsdaten>\Novell\ZENworks\Remote Management\bin` installiert.
2. Führen Sie den folgenden Befehl aus:

   ```
   nzrViewer [/Optionen<ggf. Parameter>][IP-Adresse des verwalteten Geräts]
   [~~Port]
   ```

   Der Standardport für das verwaltete Gerät ist 5950.

   Informationen zu den verfügbaren Befehlszeilenoptionen finden Sie unter Abschnitt 2.9.1, „Befehlszeilenoptionen zum Starten eines Fernvorgangs“, auf Seite 46.
3. Klicken Sie auf *Verbinden*.

   Bei erfolgreicher Authentifizierung wird die Fernsitzung gestartet. Wenn Sie in der Befehlszeile den Typ des Fernvorgangs nicht angegeben haben, wird standardmäßig eine Fernsteuerungssitzung gestartet.

Das Starten eines Fernverwaltungsvorgangs mithilfe der Befehlszeilenoptionen ist jedoch folgendermaßen eingeschränkt:

- Wenn Sie die Befehlszeilenoptionen `key`, `cert` und `CAcert` im Befehl `nzrViewer` nicht zur SSL-Authentifizierung angeben möchten, muss die Option *Verbindung zulassen, wenn Fernverwaltungskonsole über kein SSL-Zertifikat verfügt* in den Sicherheitseinstellungen der Fernverwaltungsrichtlinie aktiviert sein. Dies ist allerdings nicht zu empfehlen, da die Sicherheit des Geräts dadurch herabgesetzt wird.
- Wenn das verwaltete Gerät Teil der Verwaltungszone ist, müssen Sie sicherstellen, dass das vom Viewer zur Verfügung gestellte Zertifikat gültig, signiert und mit der Zertifizierungsstelle verkettet ist, da die SSL-Authentifizierung sonst fehlschlägt.

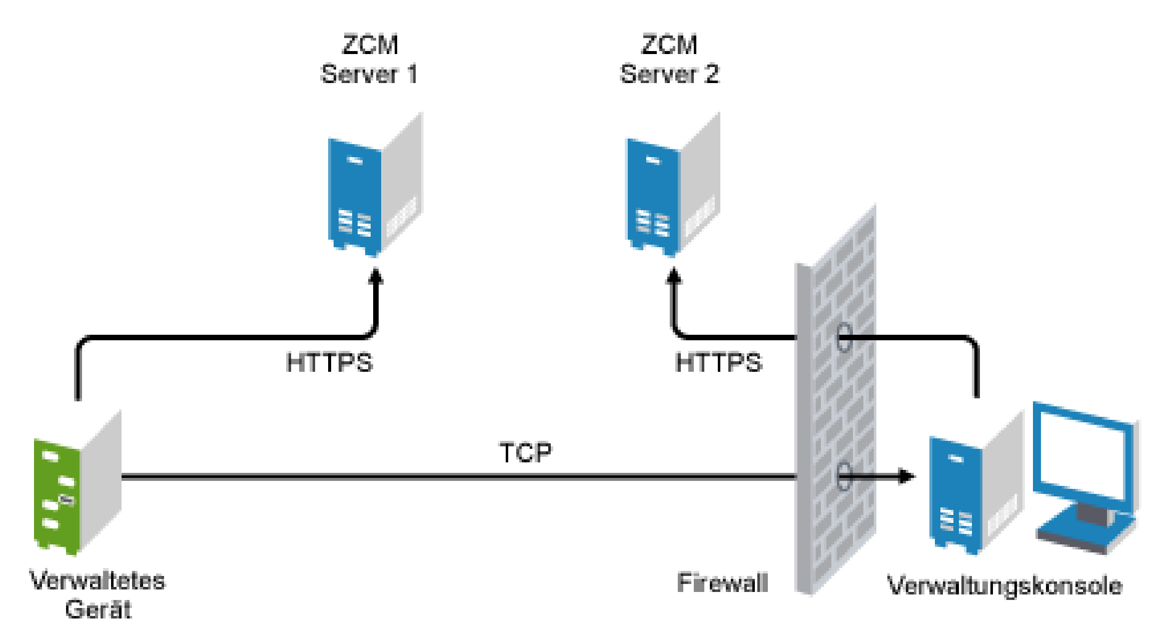
Hinweis: Wenn Sie eine Fernsitzung vom ZENworks-Kontrollzentrum (ZCC) aus starten, wird das Zertifikat automatisch vom ZCC generiert und an den Viewer zum Starten der Sitzung weitergeleitet. Das Zertifikat ist nur vier Tage gültig.

- Das vom Viewer zur Verfügung gestellte Zertifikat wird vom verwalteten Gerät zur Identifizierung des Fernoperators verwendet. Wenn vom Viewer kein Zertifikat zur Verfügung gestellt wird, wird der Benutzer nicht identifiziert und in der Berechtigungsnachricht, im visuellen Signal und in den Revisionsprotokollen als *unbekannt* erfasst.

2.8.2 Initiieren einer Sitzung über das verwaltete Gerät

In diesem Szenario wird die Fernsitzung vom Benutzer am verwalteten Gerät initiiert. Dies ist sinnvoll, wenn die Verwaltungskonsole keine Verbindung zum verwalteten Gerät herstellen kann. Die nachstehende Abbildung zeigt eine Fernsitzung, die von einem Benutzer am verwalteten Gerät initiiert wurde.

***Abbildung 2-2** Agenteninitiierte Sitzung*



Unter folgenden Bedingungen kann der Benutzer am verwalteten Gerät anfordern, dass ein Fernoperator eine Fernsitzung am Gerät durchführen soll:

- Der Fernoperator hat den Fernverwaltungs-Listener für die Überwachung der Fernsitzungsanforderungen des Benutzers gestartet.
- Die Option *Benutzern das Anfordern einer Fernsitzung ermöglichen* ist in der Fernverwaltungsrichtlinie aktiviert.
- Der Port, den der Fernverwaltungs-Listener auf Fernverbindungen überwacht, muss in der Firewall der Verwaltungskonsole geöffnet sein. Der Standardport ist 5550.

So fordern Sie eine Sitzung an:

1. Doppelklicken Sie im Benachrichtigungsbereich auf das ZENworks-Symbol.
2. Navigieren Sie im linken Fensterbereich zu *Fernverwaltung* und klicken Sie dann auf *Allgemein*.
3. Klicken Sie auf *Fernverwaltungssitzung anfordern*, um das Dialogfeld „Sitzung anfordern“ zu öffnen.

   Die Möglichkeit, eine Fernverwaltungssitzung anzufordern, wird durch Ihren Administrator gesteuert; die Option kann also deaktiviert sein, insbesondere wenn Ihre Firma oder Abteilung über kein Support-Personal verfügt, das als Fernoperator arbeitet. Wenn die Option *Fernverwaltungssitzung anfordern* nicht als Verknüpfungstext angezeigt wird, ist die Option deaktiviert.
4. Wählen Sie in der Liste *Überwachende Fernoperatoren* den Fernoperator aus, mit dem Sie die Fernsitzung starten möchten.

   oder

   Wenn der Fernoperator nicht aufgeführt ist, geben Sie die Verbindungsinformationen des Operators in die Felder unter *Verbindung anfordern* ein.
5. Wählen Sie im Feld *Aktion* den Typ des gewünschten Vorgangs aus (Fernsteuerung, Fernansicht, Ferndiagnose, Dateiübertragung oder Fernausführung).

   Weitere Informationen zu jeder Operation erhalten Sie unter Abschnitt 1.2, „Zum Verständnis von Fernverwaltungsvorgängen“, auf Seite 12.
6. Klicken Sie auf *Anfordern*, um die Sitzung zu starten.

Wenn Verbindungen von einem öffentlichen Netzwerk zu einem privaten Netzwerk zulässig sein sollen, müssen Sie das DNS Application Level Gateway (DNS_ALG) bereitstellen. Weitere Informationen zu DNS_ALG finden Sie in RFC 2694 (http://www.ietf.org/rfc/rfc2694).

2.9 Optionen zum Starten eines Fernverwaltungsvorgangs

Wenn Sie einen Fernverwaltungsvorgang über die Befehlszeile starten, können Sie das Verhalten der Fernverwaltungssitzung mittels Befehlszeilenoptionen steuern. Die Option `remotecontrol` startet zum Beispiel einen Fernsteuerungsvorgang auf dem Gerät und die Option `notoolbar` blendet die Symbolleiste im anzeigenden Fenster aus.

Die Fernverwaltung verwendet beim Starten eines Fernverwaltungsvorgangs auf einem Gerät verschiedene interne Optionen. Die Option `zenrights` gibt zum Beispiel an, dass als Authentifizierungsschema „ZENworks Rights Authentication“ (Rechteauthentifizierung von

ZENworks) verwendet wird. Diese internen Optionen sollten Sie beim Starten eines Fernverwaltungsvorgangs über die Befehlszeile nicht angeben. Weitere Informationen über die intern verwendeten Optionen finden Sie im Abschnitt 2.9.2, „Interne Optionen zum Starten eines Fernvorgangs“, auf Seite 49.

In den folgenden Abschnitten finden Sie ausführliche Informationen zu den Fernverwaltungsoptionen:

2.9.1 Befehlszeilenoptionen zum Starten eines Fernvorgangs

Mit den folgenden Befehlszeilenoptionen können Sie einen Fernverwaltungsvorgang steuern:

Tabelle 2-1 *Befehlszeilenoptionen zum Starten eines Fernvorgangs*

Befehlszeilenoption	Parameter	Beschreibung
listen	*Port*	Aktiviert den Listener für die Überwachung des angegebenen Ports auf Anforderungen für Fernsitzungen. Standardmäßig lautet die Portnummer 5550.
restricted		Blendet Symbolleiste und Systemmenü aus.
viewonly		Startet einen Fernansichtsvorgang auf dem verwalteten Gerät.
remotecontrol		Startet einen Fernsteuerungsvorgang auf dem verwalteten Gerät.
ftponly		Startet einen Dateiübertragungsvorgang auf dem verwalteten Gerät.
remoteexecute		Startet einen Fernausführungsvorgang auf dem verwalteten Gerät.
diagnostics	*appname*	Startet einen Ferndiagnosevorgang auf dem verwalteten Gerät. Bei Angabe des Parameters „appname“ wird die Anwendung auf dem verwalteten Gerät gestartet.
filecompressionlevel	*Grad*	Bietet Mittel zur Optimierung des Dateikomprimierungsprozesses für höhere Geschwindigkeit oder bessere Komprimierung während eines Dateiübertragungsvorgangs. Der Komprimierungsgrad kann im Bereich von 0 bis 9 liegen. • 0 bedeutet keine Komprimierung • 1 bedeutet höchste Geschwindigkeit • 9 bedeutet beste Komprimierung Wenn der Komprimierungsgrad nicht angegeben ist, wird der Standardkomprimierungsgrad, 6, verwendet, der eine Optimierung sowohl für Geschwindigkeit als auch für Komprimierung bedeutet.
noencrypt		Startet die Fernsitzung im unverschlüsselten Modus.
fullscreen		Startet einen Fernvorgang im Vollbildmodus auf dem verwalteten Gerät.

Befehlszeilenoption	Parameter	Beschreibung
notoolbar		Blendet die Symbolleiste des Anzeigefensters aus.
exclusive		Startet die Fernsitzung im exklusiven Modus.
8bit		Gibt die zum Rendern der Sitzungsdaten zu verwendende Farbtiefe an.
freigegeben		Aktiviert eine freigegebene Verbindung, mit der Sie den Desktop gemeinsam mit anderen Clients, die ihn bereits verwenden, nutzen können. Diese Option ist standardmäßig auf „True“ (Wahr) gesetzt.
collaborate		Startet die Fernsitzung im Zusammenarbeitsmodus. Diese Option wird auf Linux noch nicht unterstützt.
noshared		Aktiviert eine nicht freigegebene Verbindung, bei der, je nach Serverkonfiguration, die Verbindung anderer Clients getrennt oder Ihre eigene Verbindung verweigert wird.
swapmouse		Vertauscht die Maustasten.
nocursor		Zeigt nur den Mauszeiger des verwalteten Geräts an. Der lokale Mauszeiger wird nicht angezeigt.
dotcursor		Zeigt den lokalen Mauszeiger als Punkt an. Diese Option ist standardmäßig auf „True“ (Wahr) gesetzt.
smalldotcursor		Zeigt den lokalen Mauszeiger als kleinen Punkt an.
normalcursor		Zeigt den lokalen Mauszeiger in der Standardform an.
belldeiconify		Ermöglicht die Übertragung eines Bell-Zeichens, das zur Ausgabe eines Signaltons beim Viewer führt. Diese Option führt außerdem dazu, dass ein minimierter vncviewer beim Empfang des Bell-Zeichens maximiert wird.
emulate3		Benutzer mit einer Maus mit zwei Tasten können die mittlere Taste durch gleichzeitiges Drücken beider Tasten emulieren. Diese Option ist standardmäßig auf „True“ (Wahr) gesetzt.
noemulate3		Es wird keine Maus mit drei Tasten emuliert.
nojpeg		Deaktiviert verlustbehaftete JPEG-Komprimierung. Dies wird nicht empfohlen, da die Effizienz des Kodierers beeinträchtigt werden könnte. Diese Option kann verwendet werden, wenn es zwingend erforderlich ist, eine perfekte Bildqualität zu erzielen.
nocursorshape		Deaktiviert die Aktualisierungen der Cursorform zur Verarbeitung von Bewegungen des Ferncursors. Bei Verwendung von Cursorformaktualisierungen werden die Verzögerungen bei Bewegungen des Ferncursors verringert und die Bandbreitenauslastung kann enorm verbessert werden.
noremotecursor		Der Ferncursor wird nicht angezeigt.
fitwindow		Blendet die Bildlaufleiste des Anzeigefensters aus.
scale	*Prozentsatz*	Vergrößert bzw. verkleinert das Anzeigefenster auf den angegebenen Skalierungsprozentsatz.

Befehlszeilenoption	Parameter	Beschreibung
emulate3timeout	*ms*	Gibt den Zeitüberschreitungswert für die Emulierung einer Maus mit drei Tasten an.
disableclipboard		Deaktiviert das Kopieren von Daten in die Zwischenablage.
delay		Rendert einen Anzeigebereich und wartet die angegebene Zeit, bevor die nächste Aktualisierung abgerufen wird.
loglevel	*n*	Gibt den Umfang der Informationsprotokollierung an.
console		Protokolliert die Informationen in einem Konsolenfenster.
logfile	*Dateiname*	Name der Protokolldatei, in der die Informationen protokolliert werden sollen.
config	*Dateiname*	Name der Konfigurationsdatei, die zum Laden vordefinierter Konfigurationseinstellungen verwendet werden soll.
key	*Dateiname*	Name der Datei, in der der private Schlüssel gespeichert wird. Dieser Schlüssel wird während des SSL-Handshake mit dem verwalteten Gerät verwendet. **Wichtig:** Der Schlüssel und die Zertifizierungsoptionen müssen zusammen verwendet werden. Wenn Sie diese Optionen zusammen mit dem Befehl `nzrViewer` verwenden, müssen Sie aus Sicherheitsgründen die Option *Verbindung erlauben, wenn Fernverwaltungskonsole über kein SSL-Zertifikat verfügt* in den Sicherheitseinstellungen der Fernverwaltungsrichtlinie deaktivieren.
cert	*Dateiname*	Name der Datei, in der das Zertifikat für den privaten Schlüssel gespeichert wird. **Wichtig:** Der Schlüssel und die Zertifizierungsoptionen müssen zusammen verwendet werden. Wenn Sie diese Optionen zusammen mit dem Befehl `nzrViewer` verwenden, müssen Sie aus Sicherheitsgründen die Option *Verbindung erlauben, wenn Fernverwaltungskonsole über kein SSL-Zertifikat verfügt* in den Sicherheitseinstellungen der Fernverwaltungsrichtlinie deaktivieren.
CAcert	*Dateiname*	Der Name der Datei, in der das Stammzertifikat gespeichert wird. Mit diesem Zertifikat kann das Zertifikat des verwalteten Geräts während eines SSL-Handshake überprüft werden.
encoding	*Kodierungs-name*	Gibt die gewünschte Kodierung für die Sitzung an. Die verschiedenen Kodierungstypen lauten: Raw, CopyRect, RRE, CoRRE, Hextile, Zlib und Tight.

Befehlszeilenoption	Parameter	Beschreibung
compresslevel	*n*	Geben Sie den Komprimierungsgrad an, um die Daten der Fernsitzung von 0 auf 9 zu komprimieren. Bei Grad 1 wird ein Minimum an CPU-Zeit in Anspruch genommen und es werden schwache Komprimierungsraten erzielt; Grad 9 bietet die beste Komprimierung, ist jedoch langsam, was den CPU-Zeitaufwand auf der Serverseite betrifft. Verwenden Sie einen hohen Komprimierungsgrad bei sehr langsamen Netzwerkverbindungen und einen niedrigen Komprimierungsgrad bei Hochgeschwindigkeits-LAN-Verbindungen. Von der Verwendung von Komprimierungsgrad 0 wird abgeraten.
quality	*n*	Gibt die JPEG-Qualität als Stufe von 0 bis 9 an. Qualitätsstufe 0 bringt eine schlechte Bildqualität, jedoch eine enorme Komprimierungsrate mit sich; Stufe 9 dagegen eine gute Bildqualität bei einer geringeren Komprimierungsrate.
zenpasswd		Gibt an, dass als Authentifizierungsschema die ZENWorks-Passwortauthentifizierung verwendet werden soll.
Ländereinstellung		Gibt die Ländereinstellung an, in der die Ressourcen angezeigt werden sollen. Standardmäßig wird Englisch verwendet. Für diese Option kommen Englisch, Französisch, Spanisch, Portugiesisch, Japanisch, Italienisch, Chinesisch (vereinfacht) und Chinesisch (traditionell) in Frage.
Vertretung	proxy_server	Gibt den DNS-Namen oder die IP-Adresse des Fernverwaltungs-Proxys sowie die Portnummer in einem der folgenden Formate an: ◆ *IP-Adresse~~Port*. Zum Beispiel 10.0.0.0~~5750. ◆ *IP-Adresse~Port*. Zum Beispiel 10.0.0.0~50. Der Standardport für den Proxy ist 5750.

2.9.2 Interne Optionen zum Starten eines Fernvorgangs

In der folgenden Tabelle werden die von der Fernverwaltung intern verwendeten Optionen beschrieben. Diese Optionen sollten Sie beim Starten eines Fernverwaltungsvorgangs über die Befehlszeile nicht angeben.

Tabelle 2-2 *Interne Optionen zum Starten eines Fernvorgangs*

Option	Beschreibung
zenrights	Legt als Authentifizierungsschema „ZENworks Rights Authentication“ (Rechteauthentifizierung von ZENworks) fest.
pipe	Gibt die Authentifizierungsinformationen an.

2.10 Installieren eines Fernverwaltungs-Proxys

Wenn sich ein verwaltetes Gerät in einem privaten Netzwerk oder auf der anderen Seite einer Firewall oder eines Routers befindet, die/der NAT (Network Address Translation) verwendet, kann der Fernverwaltungsvorgang des Geräts durch einen Fernverwaltungs-Proxy geleitet werden. Der Proxy kann auf einem verwalteten Windows-Gerät oder auf einem Linux-Gerät (Primärserver oder Satellitenserver) installiert werden. Standardmäßig überwacht der Fernverwaltungs-Proxy Port 5750.

Weitere Informationen zum Fernverwaltungs-Proxy finden Sie im Abschnitt 1.4, „Funktionen des Fernverwaltungs-Proxys", auf Seite 16.

Informationen zu den Systemanforderungen für ein verwaltetes Windows-Gerät oder ein Linux-Gerät, auf dem der Proxy installiert werden soll, finden Sie im *ZENworks 10 Configuration Management-Installationshandbuch* im Abschnitt „Systemanforderungen".

So installieren Sie den Proxy:

Unter Windows:

1. Öffnen Sie am Gerät einen Webbrowser mit der ZENworks-Download-Seite:

   https://*server*/zenworks-setup

   wobei *Server* dem DNS-Namen oder der IP-Adresse eines ZENworks-Servers entspricht.
2. Klicken Sie im linken Navigationsbereich auf *Verwaltung*.
3. Klicken Sie auf `novell-zenworks-rm-repeater-<Version>.msi` und speichern Sie die Datei in einem temporären Verzeichnis.

   version bezeichnet die Version des ZENworks-Produkts.
4. Installieren Sie die Proxyanwendung, indem Sie den folgenden Befehl ausführen:

   ```
   msiexec /i novell-zenworks-rm-repeater-<Version>.msi
   TARGETDIR=„ZENworks_Installationsverzeichnis".
   ```

Unter Linux:

1. Öffnen Sie am Gerät einen Webbrowser mit der ZENworks-Download-Seite:

   https://*server*/zenworks-setup

   wobei *Server* dem DNS-Namen oder der IP-Adresse eines ZENworks-Servers entspricht.
2. Klicken Sie im linken Navigationsbereich auf *Verwaltung*.
3. Klicken Sie auf `novell-zenworks-rm-repeater-<Version>.noarch.rpm`.
4. Entscheiden Sie, ob der Proxy sofort installiert werden soll oder ob die RPM-Datei des Proxys für die Installation zu einem späteren Zeitpunkt gespeichert werden soll.

   - Klicken Sie zur sofortigen Installation des Proxys auf *Öffnen mit*, um den Fernverwaltungs-Proxy mit „zen-installer" zu öffnen, geben Sie das Root-Passwort an und klicken Sie anschließend auf *OK*.

- Sie können die Proxy-RPM-Datei aber auch in das beim Herunterladen vorgeschlagene Standardverzeichnis speichern, um den Proxy zu einem späteren Zeitpunkt zu installieren. Klicken Sie dazu auf *Auf Datenträger speichern*. Führen Sie eine der folgenden Aktionen aus, um die RPM-Datei zu installieren:
  - Klicken Sie auf die RPM-Datei des Proxys, geben Sie das Root-Passwort an und klicken Sie anschließend auf *OK*.
  - Führen Sie den folgenden Befehl als Superuser oder Root-Benutzer aus:

    ```
    rpm -ivh novell-zenworks-rm-repeater-<Version>.noarch.rpm
    ```

Der Fernverwaltungs-Proxy ist so konfiguriert, dass er nach seiner Installation automatisch ausgeführt wird. Sein Verhalten können Sie aber durch Änderung der Standardeinstellungen auf dem Gerät anpassen. Weitere Informationen zu den Einstellungen des Fernverwaltungs-Proxys finden Sie im Abschnitt 2.11, „Konfigurieren eines Fernverwaltungs-Proxys", auf Seite 51.

2.11 Konfigurieren eines Fernverwaltungs-Proxys

Bei der Installation des Fernverwaltungs-Proxys auf einem Gerät erhalten bestimmte Einstellungen auf dem Gerät eine Standardkonfiguration. Diese Einstellungen können Sie ändern.

2.11.1 Einstellungen des Fernverwaltungs-Proxys auf einem Windows-Gerät

Auf einem Windows-Gerät befinden sich die Registrierungseinstellungen für den Fernverwaltungs-Proxy unter dem Eintrag `HKLM\SOFTWARE\Novell\ZCM\Remote Management\Proxy`.

ClientPort: Gibt den Port an, den der Proxy auf Fernsitzungsanforderungen des Fernverwaltungs-Viewers überwacht. Der Standardwert ist 5750.

SessionEncryption: Legt fest, ob der anfängliche Datenfluss zwischen dem Proxy und dem Fernverwaltungs-Viewer verschlüsselt wird. Der Standardwert ist „Wahr". Nach der Herstellung der Verbindung zwischen Proxy und verwaltetem Gerät gilt die Einstellung nicht mehr. Ab diesem Zeitpunkt gelten die Sitzungsverschlüsselungsregeln der Fernverwaltungsrichtlinie sowie die Einstellungen des Fernoperators. Sie sollten diese Einstellung nicht ändern, da bei „False" neben dem Fernverwaltungs-Viewer auch andere nicht authentifizierte externe Prozesse Verbindungen zu Geräten innerhalb des privaten Netzwerks herstellen können.

SSLClientAuthentication: Legt fest, ob der Proxy auch Verbindungsanforderungen von Viewern akzeptiert, die über kein gültiges Zertifikat verfügen. Mögliche Werte sind „True" und „False". Der Standardwert ist „Wahr".

2.11.2 Einstellungen des Fernverwaltungs-Proxys auf einem Linux-Primär- oder -Satellitenserver

Auf einem Linux-Primär- oder -Satellitenserver befinden sich die Einstellungen für den Fernverwaltungs-Proxy in der Datei `/etc/opt/novell/zenworks/repeater/nzrepeater.ini`. Die wichtigsten dieser Einstellungen sind:

viewerport: Gibt den Port an, den der Fernverwaltungs-Proxy auf Fernsitzungsanforderungen des Fernverwaltungs-Viewers überwacht. Der Standardwert ist 5750.

runasuser: Gibt den Benutzer an, für den der Proxy ausgeführt wird. Der Fernverwaltungs-Proxy benötigt zur Ausführung von Fernvorgängen lediglich Benutzerberechtigungen. Der Standardwert ist „zenworks“. Sie können aber auch einen anderen Benutzer angeben.

strictimpersonation: Legt fest, ob die Fernsitzung als `Root` ausgeführt wird, wenn der unter „runasuser“ angegebene Benutzer nicht existiert. Mögliche Werte sind „true“ und „false“. Der Standardwert ist „false“, das heißt, die Fernsitzung wird als `Root` ausgeführt, wenn der unter „runasuser“ angegebene Benutzer nicht existiert.

sslauth: Legt fest, ob die SSL-Authentifizierung aktiviert oder deaktiviert ist. Mögliche Werte sind „0“ und „1“. Der Standardwert ist „1“, das heißt, die SSL-Authentifizierung ist aktiviert.

Warnung: Die Deaktivierung der SSL-Authentifizierung wird nicht empfohlen, da in diesem Fall externe Prozesse ohne Authentifizierung auf Netzwerkgeräte zugreifen können.

---

verifyViewerCert: Legt fest, ob die Zertifikate des Fernverwaltungs-Viewers überprüft werden müssen. Diese Einstellung tritt nur bei aktivierter SSL-Authentifizierung in Kraft. Mögliche Werte sind „0“ und „1“. Der Standardwert ist „1“, das heißt, die Zertifikate des Fernverwaltungs-Viewers müssen überprüft werden. Wenn eine Sitzung von einem Einzelplatz-Viewer initiiert wird, verfügt der Fernoperator möglicherweise nicht über die erforderlichen Zertifikate, da diese mit der Root-Zertifizierungsstelle verknüpft sind. In diesem Fall kann der Proxy keine Verbindung zum Server herstellen.

loggingenabled: Legt fest, ob die Meldungen auf dem Gerät protokolliert werden. Mögliche Werte sind „true“ und „false“. Der Standardwert ist „true“.

Informationen zu weiteren Registrierungseinstellungen finden Sie in der Datei `/etc/opt/novell/zenworks/repeater/nzrepeater.ini`.

Verwalten von Fernsitzungen

3

In den folgenden Abschnitten finden Sie Informationen zur effizienten Verwaltung von Fernverwaltungssitzungen in Novell® ZENworks® 10 Configuration Management:

3.1 Verwalten einer Fernsteuerungssitzung

Mithilfe der Fernverwaltung können Sie ein verwaltetes Gerät per Fernzugriff steuern. Mithilfe von Fernsteuerungsverbindungen kann der Fernoperator das verwaltete Gerät nicht nur anzeigen, sondern auch dessen Steuerung übernehmen. Dies ist hilfreich, um Benutzerunterstützung bereitzustellen und Probleme auf dem verwalteten Gerät zu beheben. Informationen zum Starten einer Fernsteuerungssitzung finden Sie unter Abschnitt 2.8, „Starten von Fernverwaltungsvorgängen“, auf Seite 36.

3.1.1 Verwenden der Symbolleistenoptionen im Fernverwaltungs-Viewer

In der nachfolgenden Tabelle werden die unterschiedlichen Symbolleistenoptionen erläutert, die während einer Fernsteuerungssitzung im Fernverwaltungs-Viewer zur Verfügung stehen. Außerdem werden hier ggf. die jeweiligen Tastenkombinationen aufgeführt.

Tabelle 3-1 *Symbolleistenoptionen im Fernverwaltungs-Viewer*

Option	Tastenkombination	Funktionalität
Verbindungsoptionen	Strg + Alt + Umschalt + P	Ermöglicht Ihnen die Konfiguration verschiedener Sitzungsparameter wie Format und Kodierung zur Verbesserung der Sitzungsleistung, der Protokollierung sowie der Steuerung des lokalen und entfernten Cursors.
Verbindungs-informationen	Strg + Alt + Umschalt + I	Gibt den Hostnamen, den Port, die Bildschirmauflösung und die Protokollversion des verwalteten Geräts an.

Option	Tastenkombination	Funktionalität
Vollbild	Strg + Alt + Umschalt + F	Ermöglicht Ihnen das Umschalten zwischen Vollbildmodus und normalem Modus.
Bildschirmaktualisierung anfordern	Strg + Alt + Umschalt + H	Aktualisiert das Anzeigefenster.
Strg + Alt + Entf senden		Sendet die Tastenkombination Strg + Alt + Entf an das verwaltete Gerät. Die Möglichkeit, die Funktion von Strg+Alt+Entf auf einem Windows 7-Gerät zu simulieren, ist zurzeit deaktiviert.
Strg-Esc senden		Ruft das Startmenü auf dem verwalteten Gerät auf.
Alt-Tastendruck senden		Durch Klicken auf diese Option und Drücken der Taste ALT auf der Tastatur wird der Tastaturbefehl ALT an das verwaltete Gerät gesendet.
Bildschirm ausblenden/anzeigen	Strg + Alt + Umschalt + B	Aktiviert bzw. deaktiviert die Bildschirmanzeige des verwalteten Geräts. Bei Verwendung der Bildschirmaustastung kann der Benutzer am Gerät die Vorgänge nicht sehen, die der Fernoperator auf dem Gerät ausführt. Die Steuerelemente von Tastatur und Maus für das verwaltete Gerät werden ebenfalls gesperrt. Diese Option ist nur aktiviert, wenn die Option *Bildschirmaustastung des verwalteten Geräts während Fernsteuerung zulassen* in der Fernverwaltungsrichtlinie aktiviert ist, die auf dem verwalteten Gerät wirksam ist.
Tastatur und Maus sperren/entsperren	Strg + Alt + Umschalt + L	Sperrt die Steuerelemente von Tastatur und Maus für das verwaltete Gerät oder hebt die Sperrung auf. Wenn die Maus- und Tastatursteuerung des Geräts gesperrt sind, kann der Benutzer am verwalteten Gerät diese nicht verwenden. Diese Option ist nur aktiviert, wenn die Option *Sperren von Maus und Tastatur am verwalteten Gerät während Fernsteuerung zulassen* in der Fernverwaltungsrichtlinie aktiviert ist, die auf dem verwalteten Gerät wirksam ist.

Option	Tastenkombination	Funktionalität
Dateien übertragen	Strg + Alt + Umschalt + T	Startet eine Sitzung zum Übertragen von Dateien zu und von dem verwalteten Gerät. Diese Option ist nur aktiviert, wenn die Option *Übertragung von Dateien an verwaltetes Gerät zulassen* in der Fernverwaltungsrichtlinie aktiviert ist, die auf dem verwalteten Gerät wirksam ist. Weitere Informationen zur Dateiübertragung finden Sie unter Abschnitt 3.5, „Verwalten einer Dateiübertragungssitzung“, auf Seite 60.
Zusammenarbeit		Startet eine ZENworks-Fernverwaltungs-Zusammenarbeitssitzung auf dem verwalteten Gerät, die es Ihnen ermöglicht, mehrere Fernoperatoren zur Teilnahme an der Fernverwaltungssitzung einzuladen. Sie können auch die Fernsteuerungsrechte an einen anderen Fernoperator delegieren, damit dieser Sie bei der Lösung eines Problems unterstützt. Diese Option wird zurzeit nur unter Windows unterstützt. Weitere Informationen zur Sitzungszusammenarbeit finden Sie unter Abschnitt 3.1.2, „Sitzungszusammenarbeit“, auf Seite 55.
Fernausführung	Strg + Alt + Umschalt + U	Startet eine Fernausführungssitzung auf dem verwalteten Gerät, sodass Sie jede ausführbare Datei auf dem verwalteten Gerät fernstarten können. Diese Option ist nur aktiviert, wenn die Option *Fernausführung von Programmen an verwaltetem Gerät zulassen* in der Fernverwaltungsrichtlinie aktiviert ist, die auf dem verwalteten Gerät wirksam ist.
Bildschirmschoner überschreiben	Strg + Alt + Umschalt + O	Setzt den passwortgeschützten Bildschirmschoner während der Fernsitzung auf dem verwalteten Gerät außer Kraft. Diese Option ist nur aktiviert, wenn die Option *Automatisches Entsperren des Bildschirmschoners bei Fernsteuerung zulassen* in der Fernverwaltungsrichtlinie aktiviert ist, die auf dem verwalteten Gerät wirksam ist.
Trennen	Alt+F4	Schließt die Fernsitzung.

3.1.2 Sitzungszusammenarbeit

Mit der Funktion zur Sitzungszusammenarbeit können Sie mehrere Fernoperatoren einladen, sich an der Fernverwaltungssitzung zu beteiligen, sofern die Fernoperatoren den Fernverwaltungs-Listener für die Überwachung der Anforderungen für Fernsitzungen gestartet haben. Sie können auch die Fernsteuerungsrechte an einen Fernoperator delegieren, damit dieser Sie bei der Lösung eines Problems unterstützt, und die Steuerung anschließend wieder vom Fernoperator zurückfordern. Diese Option wird zurzeit nur unter Windows unterstützt.

Wenn Sie zuerst die Fernsteuerungssitzung auf dem verwalteten Gerät starten, erhalten Sie die Privilegien des Master-Fernoperators. Mithilfe der Sitzungszusammenarbeit können Sie:

- Mehrere Fernoperatoren zur Teilnahme an der Fernsteuerungssitzung einladen
- Die Fernsteuerungsrechte an einen Fernoperator delegieren, damit dieser Sie bei der Lösung eines Problems unterstützt, und sie anschließend wieder zurückerlangen
- Eine Fernsitzung beenden.

So starten Sie eine Sitzungszusammenarbeit:

1. Starten Sie die Fernsteuerungssitzung auf dem verwalteten Gerät im Zusammenarbeitsmodus.

   Informationen zum Starten einer Fernsteuerungssitzung finden Sie hier: Abschnitt 2.8, „Starten von Fernverwaltungsvorgängen“, auf Seite 36.

2. Klicken Sie in der Symbolleiste des Fernverwaltungs-Viewers auf , um das Fenster für die Sitzungszusammenarbeit anzuzeigen.

Im Fenster für die Sitzungszusammenarbeit sind alle Fernoperatoren aufgelistet, die in der auf dem Gerät wirksamen Fernverwaltungsrichtlinie hinzugefügt wurden. Jeder Fernoperator wird als separater Eintrag aufgeführt, vor dem ein farbiger Kreis angezeigt wird:

- Ein grauer Kreis gibt an, dass sich der Fernoperator nicht bei der Sitzung angemeldet hat.
- Ein roter Kreis gibt an, dass sich der Fernoperator bei der Sitzung angemeldet hat und sich im Fernansichtsmodus befindet.
- Ein grüner Kreis bedeutet, dass der Fernoperator sich bei der Sitzung angemeldet hat und Fernsteuerungsrechte für die Sitzung an ihn delegiert wurden.

Weitere Informationen zum Hinzufügen von Fernoperatoren finden Sie unter „Abschnitt 2.3, „Erstellen der Fernverwaltungsrichtlinie“, auf Seite 23“.

In der folgenden Tabelle sind die Aktionen aufgeführt, die Sie während einer Sitzungszusammenarbeit als Master-Fernoperator ausführen können:

Tabelle 3-2 *Optionen im Fenster für die Sitzungszusammenarbeit*

Aufgabe	Vorgehensweise	Zusätzliche Details
Fernoperator zur Teilnahme an einer Fernsitzung einladen	1. Wählen Sie einen Fernoperator aus, der im Fenster für die Sitzungszusammenarbeit aufgeführt ist. 2. Klicken Sie auf *Einladen*.	Wenn der Fernoperator die Anforderung akzeptiert und sich bei der Sitzung anmeldet, wird der graue Kreis für den Fernoperator in einen roten Kreis geändert. Die neue Sitzung wird standardmäßig im Modus „Fernansicht“ gestartet.

Aufgabe	Vorgehensweise	Zusätzliche Details
Fernsteuerungsrechte an einen Fernoperator delegieren	1. Wählen Sie den Fernoperator aus, an den Sie die Fernsteuerungsrechte delegieren möchten. 2. Klicken Sie auf *Delegieren*.	Der ausgewählte Fernoperator befindet sich jetzt im Fernsteuerungsmodus und der rote Kreis für den Fernoperator wird in einen grünen Kreis geändert. Der Master-Fernoperator wechselt automatisch in den Fernansichtsmodus.
Fernsteuerungsrechte von einem Fernoperator wiedererlangen	1. Klicken Sie auf *Steuerung wiedererlangen*.	Der Fernoperator wechselt in den Fernansichtsmodus und der grüne Kreis für den Fernoperator wird in einen roten Kreis geändert. Der Master-Fernoperator wechselt automatisch in den Fernsteuerungsmodus.
Fernsitzung beenden	1. Wählen Sie den Fernoperator aus, für den Sie die Fernsitzung beenden möchten. 2. Klicken Sie auf *Beenden*.	Wenn sich der ausgewählte Fernoperator im Fernsteuerungsmodus befindet, erlangen Sie die Fernsteuerungsrechte zurück. Die Sitzung des Fernoperators wird beendet und die Farbe des Kreises für den Fernoperator wird in grau geändert.
Externen Fernoperator einladen	1. Klicken Sie auf *Externen Fernoperator einladen*, um Fernoperatoren, die nicht im Fenster für die Sitzungszusammenarbeit aufgeführt sind, zur Teilnahme an der Fernsitzung einzuladen. 2. Geben Sie den DNS-Namen oder die IP-Adresse des Geräts des Fernoperators und die Portnummer an. Zum Beispiel: 10.0.0.0 ~~1000. 3. Klicken Sie auf *Einladen*.	

Wenn der Master-Fernoperator die Fernsitzung verlässt, wird die Sitzung für alle Fernoperatoren beendet.

3.2 Verwalten einer Fernansichtssitzung

Mit der Funktion für die Fernansicht können Sie eine Fernverbindung zu einem verwalteten Gerät herstellen, sodass Sie den Desktop des verwalteten Geräts anzeigen können. Informationen zum Starten einer Fernansichtssitzung finden Sie unter Abschnitt 2.8, „Starten von Fernverwaltungsvorgängen“, auf Seite 36.

In der nachfolgenden Tabelle werden die unterschiedlichen Symbolleistenoptionen erläutert, die während einer Fernansichtssitzung im Fernverwaltungs-Viewer zur Verfügung stehen.

Tabelle 3-3 *Symbolleistenoptionen im Fernverwaltungs-Viewer*

Option	Tastenkombination	Funktionalität
Verbindungsoptionen	Strg + Alt + Umschalt + P	Ermöglicht Ihnen die Konfiguration verschiedener Sitzungsparameter wie Format und Kodierung zur Verbesserung der Sitzungsleistung, der Protokollierung sowie der Steuerung des lokalen und entfernten Cursors.
Verbindungs-informationen	Strg + Alt + Umschalt + I	Gibt den Hostnamen, den Port, die Bildschirmauflösung und die Protokollversion des verwalteten Geräts an.
Vollbild	Strg + Alt + Umschalt + F	Ermöglicht Ihnen das Umschalten zwischen Vollbildmodus und normalem Modus.
Bildschirmaktuali-sierung anfordern	Strg + Alt + Umschalt + H	Aktualisiert das Anzeigefenster.
Trennen 	Alt+F4	Schließt die Fernsitzung.

3.3 Verwalten einer Fernausführungssitzung

Mit der Funktion für die Fernausführung können Sie ausführbare Dateien auf dem verwalteten Gerät mit Systemprivilegien ausführen. Starten Sie zum Ausführen einer Anwendung auf dem verwalteten Gerät eine Fernausführungssitzung.

1 Starten Sie die Fernausführungssitzung.

Informationen zum Starten einer Fernausführungssitzung finden Sie unter Abschnitt 2.8, „Starten von Fernverwaltungsvorgängen“, auf Seite 36.

2 Geben Sie den Namen der ausführbaren Datei an.

Wenn sich die Anwendung nicht im Systempfad des verwalteten Geräts befindet, müssen Sie den vollständigen Pfad der Anwendung angeben. Wenn Sie die Erweiterung der Datei, die Sie auf dem verwalteten Gerät ausführen möchten, nicht angeben, wird automatisch die Erweiterung `.exe` angefügt.

3 Klicken Sie auf *Ausführen*.

Die Fernausführung der angegebenen Anwendung ist nicht möglich, wenn sich die Anwendung auf dem verwalteten Gerät nicht im definierten Pfad befindet.

Warnung: Das Fernverwaltungsmodul wird auf dem verwalteten Gerät standardmäßig als Dienst mit Systemprivilegien ausgeführt. Daher werden auch alle Anwendungen, die während einer Fernausführungssitzung gestartet werden, mit Systemprivilegien ausgeführt. Aus Sicherheitsgründen wird dringend empfohlen, die Anwendung nach der Verwendung zu schließen.

3.4 Verwalten einer Ferndiagnosesitzung

Mit der Funktion für die Fernverwaltung können Sie auf dem verwalteten Gerät aufgetretene Probleme Per Fernzugriff diagnostizieren und analysieren. Hiermit können Sie die Zeiten für die Problemlösung verkürzen und Benutzern Unterstützung bieten, ohne das jeweilige Gerät aufzusuchen. Dadurch wird die Benutzerproduktivität erhöht, da auf den Desktops ohne Unterbrechung weitergearbeitet werden kann.

Wenn Sie auf dem verwalteten Gerät eine Ferndiagnosesitzung starten, können Sie nur auf die Diagnoseanwendungen zugreifen, die in der Fernverwaltungseinstellung auf dem Gerät für die Diagnose und das Beheben von Problemen konfiguriert sind. Während der Sitzung werden die Diagnoseanwendungen als Symbole in einer Symbolleiste angezeigt. Die folgenden Diagnoseanwendungen sind standardmäßig in den Fernverwaltungseinstellungen konfiguriert:

***Tabelle 3-4** Symbolleistenoptionen im Fernverwaltungs-Viewer*

Option	Tastenkombination	Funktionalität
Verbindungsoptionen	Strg + Alt + Umschalt + P	Ermöglicht Ihnen die Konfiguration verschiedener Sitzungsparameter wie Format und Kodierung zur Verbesserung der Sitzungsleistung, der Protokollierung sowie der Steuerung des lokalen und entfernten Cursors.
Verbindungs-informationen	Strg + Alt + Umschalt + I	Gibt den Hostnamen, den Port, die Bildschirmauflösung und die Protokollversion des verwalteten Geräts an.
Vollbild	Strg + Alt + Umschalt + F	Ermöglicht Ihnen das Umschalten zwischen Vollbildmodus und normalem Modus.
Bildschirmaktualisierung anfordern	Strg + Alt + Umschalt + H	Aktualisiert das Anzeigefenster.

Option	Tastenkombination	Funktionalität
Dateien übertragen	Strg + Alt + Umschalt + T	Startet eine Sitzung zum Übertragen von Dateien zu und von dem verwalteten Gerät. Diese Option ist nur aktiviert, wenn die Option *Übertragung von Dateien an verwaltetes Gerät zulassen* in der Fernverwaltungsrichtlinie aktiviert ist, die auf dem verwalteten Gerät wirksam ist. Weitere Informationen zur Dateiübertragung finden Sie unter Abschnitt 3.5, „Verwalten einer Dateiübertragungssitzung“, auf Seite 60.
Trennen	Alt+F4	Schließt die Fernsitzung.

Tabelle 3-5 *Ferndiagnoseanwendungen*

Symbol	Anwendung
	Systeminformationen
	Computerverwaltung
	Services
	Registrierungseditor

Sie können die Anwendungen konfigurieren, die während der Ferndiagnosesitzung auf dem verwalteten Gerät gestartet werden. Weitere Informationen zur Konfiguration der Diagnoseanwendungen finden Sie unter Abschnitt 2.1, „Konfigurieren der Fernverwaltungseinstellungen“, auf Seite 19.

3.5 Verwalten einer Dateiübertragungssitzung

Mithilfe der Fernverwaltung können Sie Dateien zwischen der Verwaltungskonsole und dem verwalteten Gerät übertragen. Informationen zum Starten einer Dateiübertragungssitzung finden Sie unter Abschnitt 2.8, „Starten von Fernverwaltungsvorgängen“, auf Seite 36.

Die Kontrollleiste „Lokaler Computer“ im Fenster „Dateiübertragung“ enthält alle Dateien und Ordner, die sich auf der Verwaltungskonsole befinden, und die Kontrollleiste „Entfernter Computer“ zeigt alle Dateien und Ordner an, die sich im Verzeichnis befinden, das über die Option

Stammverzeichnis bei Dateiübertragung in der Fernverwaltungsrichtlinie festgelegt ist. Wenn das *Stammverzeichnis bei Dateiübertragung* in der Richtlinie nicht angegeben ist oder dem verwalteten Gerät keine Richtlinie zugewiesen ist, können Sie Dateiübertragungen im gesamten Dateisystem des entfernten Geräts durchführen.

In der folgenden Tabelle werden die Steuerelemente für die Dateiübertragung und die Optionen erläutert, die für die Arbeit mit Dateien im dem Fenster „Dateiübertragung“ zur Verfügung stehen. Die Menüoption *Aktionen* wird unter Linux noch nicht unterstützt. Sie können die gewünschte Aktion jedoch über das entsprechende Symbol in der Symbolleiste ausführen.

Tabelle 3-6 *Optionen im Fenster „Dateiübertragung“*

Aufgaben	Schnelltasten	Vorgehensweise	Zusätzliche Details
Neuen lokalen Ordner erstellen	Alt+L	1. Wählen Sie die Optionsfolge *Aktionen > Neuer lokaler Ordner*. oder Klicken Sie im Bereich „Lokaler Computer“ auf . 2. Folgen Sie den Anweisungen auf dem Bildschirm.	
Neuen entfernten Ordner erstellen	Alt+W	1. Wählen Sie die Optionsfolge *Aktionen > Neuer entfernter Ordner*. oder Klicken Sie im Bereich „Entfernter Computer“ auf . 2. Folgen Sie den Anweisungen auf dem Bildschirm.	
Datei öffnen		1. Doppelklicken Sie auf die Datei, um sie in der zugeordneten Anwendung zu öffnen.	

Aufgaben	Schnelltasten	Vorgehensweise	Zusätzliche Details
Dateien oder Ordner umbenennen	Alt+N	1. Wählen Sie die Dateien oder Ordner aus, die umbenannt werden sollen. 2. Wählen Sie die Optionsfolge *Aktionen > Umbenennen*. oder Klicken Sie auf . 3. Folgen Sie den Anweisungen auf dem Bildschirm.	
Dateien oder Ordner löschen	Alt + D	1. Wählen Sie die Dateien oder die Ordner aus, die gelöscht werden sollen. 2. Klicken Sie auf *Aktionen > Löschen*. oder Klicken Sie auf 3. Folgen Sie den Anweisungen auf dem Bildschirm.	Mithilfe der Umschalt- und Strg-Taste können Sie mehrere Dateien auswählen.
Lokalen Ordner aktualisieren	Alt+E	1. Wählen Sie die Optionsfolge *Aktionen > Lokalen Ordner aktualisieren*. oder Klicken Sie im Bereich „Lokaler Computer“ auf .	
Entfernten Ordner aktualisieren	Alt+M	1. Wählen Sie die Optionsfolge *Aktionen > Entfernten Ordner aktualisieren*. oder Klicken Sie im Bereich „Entfernter Computer“ auf .	

Aufgaben	Schnelltasten	Vorgehensweise	Zusätzliche Details
Lokale Dateien sortieren		1. Wählen Sie die Optionsfolge *Aktionen > Lokal sortieren*. 2. Wählen Sie den Sortierungstyp aus. Sie können die Dateien nach Name, Größe oder Datum sortieren.	Sie können die Dateien auch sortieren, indem Sie auf die entsprechenden Spaltenüberschriften klicken.
Entfernte Dateien sortieren		1. Wählen Sie die Optionsfolge *Aktionen > Entfernt sortieren*. 2. Wählen Sie den Sortierungstyp aus. Sie können die Dateien nach Name, Größe oder Datum sortieren	Sie können die Dateien auch sortieren, indem Sie auf die entsprechenden Spaltenüberschriften klicken.
Dateien/Ordner heraufladen		1. Wählen Sie die Dateien aus, die auf den entfernten Computer heraufgeladen werden sollen. 2. Wählen Sie den Zielordner in der Kontrollleiste „Entfernter Computer“ aus. 3. Wählen Sie die Optionsfolge *Aktionen > Heraufladen*. oder Klicken Sie auf ➡	Die Option *Aktion > Heraufladen* ist nur verfügbar, wenn der lokale Computer ausgewählt ist. Mithilfe der Umschalt- und Strg-Taste können Sie mehrere Dateien auswählen.
Dateien/Ordner herunterladen	Alt+O	1. Wählen Sie die Dateien aus, die auf den entfernten Computer heruntergeladen werden sollen. 2. Wählen Sie den Zielordner in der Kontrollleiste „Lokaler Computer“ aus. 3. Wählen Sie die Optionsfolge *Aktionen > Herunterladen*. oder Klicken Sie auf ⬅	Die Option *Aktion > Herunterladen* ist nur verfügbar, wenn der entfernte Computer ausgewählt ist. Mithilfe der Umschalt- und Strg-Taste können Sie mehrere Dateien auswählen.

Aufgaben	Schnelltasten	Vorgehensweise	Zusätzliche Details
Abbrechen der Dateiübertragung	Alt+C	1. Klicken Sie auf *Aktionen* > *Dateiübertragung abbrechen*.	Sie können die Dateiübertragung auch abbrechen, indem Sie auf die Schaltfläche „Abbrechen“ klicken.
Dateieigenschaften anzeigen	Alt+P	1. Wählen Sie die Dateien aus. 2. Wählen Sie die Optionsfolge *Aktionen* > *Eigenschaften*. oder Klicken Sie auf	Mithilfe der Umschalt- und Strg-Taste können Sie mehrere Dateien auswählen. Hiermit wird die Gesamtgröße der ausgewählten Dateien und Ordner angezeigt.
In übergeordneten Ordner verschieben		1. Klicken Sie auf , um Elemente in den übergeordneten Ordner zu verschieben.	

3.6 Verwalten einer Fernverwaltungs-Proxy-Sitzung

Ein Fernverwaltungs-Proxy ermöglicht die Ausführung von Fernverwaltungsvorgängen auf verwalteten Geräten, die sich in einem privaten Netzwerk oder auf der anderen Seite einer Firewall oder eines Routers befinden, die/der NAT (Network Address Translation) verwendet.

Weitere Informationen zum Fernverwaltungs-Proxy finden Sie im Abschnitt 1.4, „Funktionen des Fernverwaltungs-Proxys“, auf Seite 16.

Informationen zur Installation eines Fernverwaltungs-Proxys finden Sie im Abschnitt 2.10, „Installieren eines Fernverwaltungs-Proxys“, auf Seite 50.

Informationen zur Konfiguration eines Fernverwaltungs-Proxys finden Sie im Abschnitt 2.11, „Konfigurieren eines Fernverwaltungs-Proxys“, auf Seite 51.

3.7 Reaktivieren eines entfernten Geräts

Mit der Fernreaktivierung können Sie einen einzelnen Knoten oder eine Gruppe von deaktivierten Knoten in Ihrem Netzwerk per Fernzugriff reaktivieren (vorausgesetzt, auf der Netzwerkkarte im Knoten ist Wake-on-LAN aktiviert).

Die Reaktivierung eines Geräts, auf dem mehrere NICs (Network Interface Cards) installiert sind, ist nur erfolgreich, wenn ein oder mehrere der NICs für das Teilnetz konfiguriert sind, in dem sich das Gerät befindet, von dem das Wake-on-LAN-Paket verteilt wird.

3.7.1 Voraussetzungen

Vor dem Reaktivieren der verwalteten Geräte müssen folgende Voraussetzungen erfüllt sein:

- Vergewissern Sie sich, dass Wake-on-LAN von der Netzwerkkarte des verwalteten Geräts unterstützt wird. Stellen Sie außerdem sicher, dass Sie die Option für Wake-on-LAN im BIOS-Setup des verwalteten Geräts aktiviert haben.
- Stellen Sie sicher, dass das verwaltete Gerät in der ZENworks-Verwaltungszone registriert wurde.
- Vergewissern Sie sich, dass sich der Fernknoten im Standby-Modus befindet. Im Standby-Modus ist die CPU ausgeschaltet und die Netzwerkschnittstellenkarte benötigt lediglich eine minimale Energiezufuhr. Die Stromverbindung zum Computer bleibt im Standby-Modus eingeschaltet, wenn der Computer heruntergefahren ist.

3.7.2 Reaktivieren der verwalteten Geräte per Fernzugriff

So führen Sie eine Fernreaktivierung durch:

1. Klicken Sie im ZENworks-Kontrollzentrum auf *Geräte*.
2. Klicken Sie auf *Server* bzw. *Arbeitsstationen*, um die Liste der verwalteten Geräte anzuzeigen.
3. Wählen Sie das Gerät aus, das reaktiviert werden soll.
4. Klicken Sie auf *Schnellaufgaben* > *Reaktivieren*, um das Dialogfeld „Reaktivieren" anzuzeigen.
5. Wählen Sie eine der folgenden Optionen aus, um die Server anzugeben, die eine Reaktivierungsanforderung an die verwalteten Geräte senden sollen.
   - **Server automatisch erkennen:** ZENworks erkennt den nächstgelegenen Primärserver des verwalteten Geräts automatisch. Wenn sich der Server und das fernverwaltete Gerät in unterschiedlichen Teilnetzen befinden, achten Sie darauf, dass der Router, der die beiden verbindet, die teilnetzorientierten Sendungen über den UDP-Port 1761 weiterleitet.
   - **Verwenden Sie die folgenden Geräte:** Klicken Sie auf *Hinzufügen*, um ein Proxy-Gerät auszuwählen, das sich im selben Teilnetz wie das Gerät befindet, das Sie reaktivieren möchten.

     Ist der Router so konfiguriert, dass teilnetzorientierte Sendungen über UDP-Port 1761 weitergeleitet werden, ist kein Proxy erforderlich.
6. (Optional) Wählen Sie eine der folgenden Optionen aus, um die IP-Adresse anzugeben, die zum Senden des Reaktivierungs-Broadcast verwendet werden soll:
   - **IP-Adresse automatisch erkennen:** ZENworks erkennt automatisch die Standard-Broadcast-Adresse des Teilnetzes, um den Reaktivierungs-Broadcast an das verwaltete Gerät zu senden.
   - **Folgende IP-Adresse verwenden:** Geben Sie die IP-Adresse an, um den Reaktivierungs-Broadcast an das verwaltete Gerät zu senden, und klicken Sie dann auf *Hinzufügen*.
7. Geben Sie in der Option *Anzahl der Wiederholungen* die Anzahl der Versuche an, die zur Reaktivierung des Geräts unternommen werden sollen. Die Standardeinstellung ist 1.
8. Geben Sie unter *Zeitabstand zwischen Wiederholungen* den Zeitraum an, der zwischen zwei Wiederholungsversuchen liegen soll. Die Standardeinstellung ist 2 Minuten.
9. Klicken Sie auf *OK*.

Die Standardwerte für die Optionen *Anzahl der Wiederholungen* und „Zeitabstand zwischen Wiederholungen" werden auf der Zonenebene konfiguriert. Sie können diese Werte auf der Geräteebene außer Kraft setzen.

3.8 Erhöhen der Fernsteuerungsleistung

Die Leistung von „Fernverwaltung" während einer Fernsitzung über eine langsame oder eine schnelle Verbindung ist vom Netzwerkverkehr abhängig. Zur Verbesserung der Antwortzeit sollten Sie mindestens eine der folgenden Aktionen ausführen:

- Abschnitt 3.8.1, „Auf der Verwaltungskonsole", auf Seite 66
- Abschnitt 3.8.2, „Auf dem verwalteten Gerät", auf Seite 66

3.8.1 Auf der Verwaltungskonsole

Klicken Sie im Fenster „ZENworks-Fernverwaltungsverbindung" auf der Konsole auf *Optionen* und legen Sie die folgenden Werte fest:

- So optimieren Sie die Fernverwaltungsleistung über eine langsame Verbindung:
  - Wählen Sie die Option *8-Bit-Farbe verwenden*.
  - Legen Sie *Benutzerdef. Komprimierungsgrad* auf Stufe 6 fest.
- Wählen Sie die Option *Mausbewegungsereignisse blockieren*.
- Aktivieren Sie die Option *Bildschirmhintergrund unterdrücken* in den Fernverwaltungseinstellungen.

3.8.2 Auf dem verwalteten Gerät

- Die Geschwindigkeit der Fernverwaltungssitzung hängt von der Prozessorleistung des verwalteten Geräts ab. Die Verwendung von Pentium* III, 700MHz (oder höher) mit mindestens 256 MB RAM wird empfohlen.
- Verwenden Sie kein Hintergrundbild mit Muster.

Sicherheit

4

Die folgenden Abschnitte enthalten sicherheitsbezogene Informationen, die Sie beachten sollten, wenn Sie die Fernverwaltungskomponente von Novell® ZENworks® 10 Configuration Management verwenden:

4.1 Authentifizierung

Der Fernverwaltungsdienst muss auf einem Gerät installiert sein, damit der Fernoperator das Gerät per Fernzugriff verwalten kann. Der Dienst wird automatisch gestartet, wenn das verwaltete Gerät gestartet wird. Wenn ein Fernoperator eine Fernsitzung auf dem verwalteten Gerät einleitet, startet der Dienst die Fernsitzung nur dann, wenn der Fernoperator zur Ausführung von Fernverwaltungsvorgängen auf dem verwalteten Gerät berechtigt ist.

Zur Verhinderung eines unbefugten Zugriffs auf das verwaltete Gerät verwendet der Fernverwaltungsdienst auf dem verwalteten Gerät die folgenden Authentifizierungsmodi:

4.1.1 Rechtsbasierte Authentifizierung für die Fernverwaltung

Bei der rechtsbasierten Authentifizierung werden dem Fernoperator Rechte zum Starten einer Fernsitzung auf dem verwalteten Gerät erteilt. Der ZENworks-Administrator und der Superadministrator verfügen standardmäßig über Rechte zur Durchführung von Fernverwaltungsvorgängen auf allen verwalteten Geräten, unabhängig davon, ob der lokale Benutzer oder der ZENworks-Benutzer beim Gerät angemeldet ist.

Der Fernoperator benötigt keine exklusiven Rechte zur Durchführung einer Fernsitzung auf dem verwalteten Gerät, wenn sich kein Benutzer beim verwalteten Gerät angemeldet hat oder wenn sich ein Benutzer beim verwalteten Gerät aber nicht bei ZENworks angemeldet hat. Der Fernoperator benötigt jedoch exklusive Fernverwaltungsrechte, um den Fernvorgang auf dem verwalteten Gerät auszuführen, wenn sich ein ZENworks-Benutzer beim Gerät angemeldet hat. Die Verwendung der rechtsbasierten Authentifizierung wird dringend empfohlen, da sie die sicherste Methode darstellt.

Für die Verwendung der berechtigungsbasierten Authentifizierung muss der ZENworks Adaptive Agent auf dem Gerät installiert sein. Es ist nicht ausreichend, nur den Fernverwaltungsdienst auf dem Gerät zu installieren.

Dieser Authentifizierungsmodus wird nicht unterstützt, wenn der Fernverwaltungsvorgang im Einzelplatzmodus oder von der Befehlszeile gestartet wird.

4.1.2 Passwortbasierte Authentifizierung für die Fernverwaltung

Bei der passwortbasierten Authentifizierung wird der Fernoperator zur Eingabe eines Passworts aufgefordert, um die Fernsitzung auf dem verwalteten Gerät zu starten.

Die zwei verfügbaren Passwortauthentifizierungsschemas sind:

- **ZENworks-Passwort:** Dieses Schema basiert auf dem SRP-Protokoll (Secure Remote Password-Protokoll) (Version 6a). Die maximale Länge eines ZENworks-Passworts beträgt 255 Zeichen.
- **VNC-Passwort:** Dies ist das traditionelle VNC-Passwortauthentifizierungsschema. Die maximale Länge eines VNC-Passworts beträgt 8 Zeichen. Dieses Passwortschema ist an sich nicht sehr sicher und wird nur für die Interoperabilität mit Open Source-Komponenten bereitgestellt.

Es wird dringend empfohlen, bei Verwendung der passwortbasierten Authentifizierung das ZENworks-Passwortschema zu verwenden, da es sicherer ist als das VNC-Passwortschema.

Die Passwortschemas arbeiten in den folgenden Modi:

- **Sitzungsmodus:** Das in diesem Modus festgelegte Passwort gilt nur für die aktuelle Sitzung. Der Benutzer des verwalteten Geräts muss am Anfang der Fernsitzung ein Passwort festlegen und es dem Fernoperator über ein bandexternes Mittel (z. B. per Telefon) mitteilen. Bei Einleitung einer Fernsitzung mit dem verwalteten Gerät muss der Fernoperator das richtige Passwort in das eingeblendete Passwortdialogfeld eingeben. Wenn der Fernoperator das richtige Passwort nicht innerhalb von zwei Minuten nach Einblendung des Dialogfelds eingibt, wird die Sitzung aus Sicherheitsgründen beendet. Bei Verwendung der passwortbasierten Authentifizierung wird dringend empfohlen, diesen Authentifizierungsmodus zu verwenden, da das Passwort nur für die aktuelle Sitzung gilt und nicht auf dem verwalteten Gerät gespeichert wird.
- **Dauerhafter Modus:** In diesem Modus kann das Passwort vom Administrator über die Fernverwaltungsrichtline oder vom Benutzer des verwalteten Geräts über das ZENworks-Symbol festgelegt werden, wenn die Option *Benutzer darf Standardpasswörter auf verwaltetem Gerät überschreiben* in den Sicherheitseinstellungen der Fernverwaltungsrichtline ausgewählt ist.

  Wenn das Passwort sowohl vom Benutzer des verwalteten Geräts als auch in der Richtlinie festgelegt wird, hat das Passwort des Benutzers Vorrang vor dem in der Richtlinie konfigurierten Passwort.

  Der Administrator kann verhindern, dass der Benutzer des verwalteten Geräts das Passwort festlegt, und kann das vom Benutzer festgelegte Passwort auch zurücksetzen, um sicherzustellen, dass während der Authentifizierung stets das Passwort verwendet wird, das in

der Richtlinie konfiguriert ist. Weitere Informationen zum Zurücksetzen des Passworts, das vom Benutzer des verwalteten Geräts festgelegt wurde, finden Sie unter Abschnitt 2.5.3, „Löschen des Fernverwaltungspassworts über das ZENworks-Kontrollzentrum“, auf Seite 33.

4.2 Sicherheit des Passworts

Verwenden Sie sichere Passwörter. Beachten Sie dabei die folgenden Richtlinien:

- **Länge:** Die empfohlene Mindestlänge beträgt 6 Zeichen. Ein sicheres Passwort verfügt über mindestens 8 Zeichen; je länger das Passwort desto besser. Die maximale Länge beträgt 255 Zeichen für ein ZENworks-Passwort und 8 Zeichen für ein VNC-Passwort.
- **Komplexität:** Ein sicheres Passwort besteht aus einer Kombination von Buchstaben und Zahlen. Es sollte Groß- und Kleinbuchstaben und mindestens eine Zahl enthalten. Durch das Hinzufügen von Zahlen zu Passwörtern, besonders in der Mitte und nicht nur am Anfang oder am Ende, kann die Sicherheit des Passworts erhöht werden. Sonderzeichen wie &, *, $ und > können die Sicherheit eines Passworts stark erhöhen. Verwenden Sie keine erkennbaren Wörter wie Eigennamen oder Wörter aus einem Wörterbuch und auch keine persönlichen Informationen wie Telefonnummern, Geburtsdaten, Jahrestage, Adressen oder Postleitzahlen.

4.3 Ports

Der Fernverwaltungsdienst wird standardmäßig an Port 5950 und der Fernverwaltungs-Listener an Port 5550 ausgeführt. Die Firewall ist bereits so konfiguriert, dass jeder vom Fernverwaltungsdienst verwendete Port zugelassen wird, Sie müssen jedoch die Firewall konfigurieren, um den vom Fernverwaltungs-Listener verwendeten Port zuzulassen.

Standardmäßig überwacht der Fernverwaltungs-Proxy Port 5750.

4.4 Revision

ZENworks Configuration Management verwaltet ein Protokoll aller Fernsitzungen, die auf dem verwalteten Gerät durchgeführt werden. Dieses Protokoll ist auf dem verwalteten Gerät gespeichert und kann vom Benutzer und vom Administrator angezeigt werden. Der Administrator kann die Protokolle aller Fernsitzungen anzeigen, die auf dem Gerät durchgeführt wurden. Der Benutzer kann die Protokolle aller Fernsitzungen anzeigen, die auf dem Gerät ausgeführt wurden, während er angemeldet war.

So zeigen Sie das Revisionsprotokoll an:

1. Doppelklicken Sie im Benachrichtigungsbereich des verwalteten Geräts auf das ZENworks-Symbol.
2. Wechseln Sie in der linken Kontrollleiste zu *Fernverwaltung* und klicken Sie dann auf *Sicherheit*.
3. Klicken Sie auf *Prüfinformationen anzeigen*, um die Prüfinformationen der Fernverwaltungsvorgänge anzuzeigen, die auf dem Gerät durchgeführt wurden.

Feld	Beschreibung
ZENworks-Benutzer	Name des ZENworks-Benutzers, der zu Beginn der Fernsitzung auf dem verwalteten Gerät angemeldet ist.

Feld	Beschreibung
Fernoperator	Name des Fernoperators, der diesen Vorgang durchgeführt hat.
Konsolenrechner	Hostname des Geräts, von dem aus der Fernvorgang ausgeführt wurde.
Konsolen-IP	IP-Adresse des Geräts, von dem aus der Fernvorgang ausgeführt wurde. **Hinweis:** Wenn der Fernverwaltungsvorgang auf dem Gerät durch einen Fernverwaltungs-Proxy weitergeleitet wird, wird die IP-Adresse des den Proxy ausführenden Geräts angezeigt.
Vorgang	Der Typ des ausgeführten Vorgangs: Fernsteuerung, Fernausführung, Fernansicht, Ferndiagnose oder Dateiübertragung.
Startzeit	Die Zeit, zu der der Fernvorgang gestartet wurde.
Endzeit	Die Zeit, zu der der Fernvorgang beendet wurde.
Status	Der Status des Fernvorgangs: Erfolgreich, wird ausgeführt oder Fehler. Die Ursache für den Fehler wird ebenfalls angezeigt.

4.5 Einholen der Erlaubnis des Benutzers am verwalteten Gerät

Der Administrator kann die Fernverwaltungsrichtlinie so konfigurieren, dass Fernoperatoren die Erlaubnis des Benutzers am verwalteten Gerät einholen müssen, bevor sie einen Fernvorgang auf dem Gerät starten.

Wenn der Fernoperator eine Fernsitzung auf dem verwalteten Gerät einleitet, überprüft der Fernverwaltungsdienst, ob die Option *Erlaubnis des Benutzers am verwalteten Gerät einholen* für diesen Fernvorgang in der auf dem Gerät wirksamen Richtlinie aktiviert ist. Wenn die Option aktiviert ist, aber kein Benutzer auf dem Gerät angemeldet ist, wird die Fernsitzung fortgesetzt. Wenn die Option jedoch aktiviert ist und sich ein Benutzer auf dem verwalteten Gerät angemeldet hat, wird eine in der Fernverwaltungsrichtlinie konfigurierte Meldung angezeigt, in der der Benutzer nach der Erlaubnis zum Starten einer Fernsitzung auf dem Gerät gefragt wird. Die Sitzung wird nur gestartet, wenn der Benutzer die Erlaubnis erteilt.

4.6 Abnormale Beendigung

Wenn eine Fernsitzung plötzlich beendet wird, wird je nach Konfiguration in den Sicherheitseinstellungen der Fernverwaltungsrichtlinie das verwaltete Gerät durch die Funktion für abnormale Beendigung gesperrt oder der Benutzer auf dem verwalteten Gerät abgemeldet. Eine Fernsitzung wird unter folgenden Umständen abnormal beendet:

- Das Netzwerk fällt aus und der Fernverwaltungs-Viewer und der Fernverwaltungsdienst können nicht mehr kommunizieren.
- Der Fernverwaltungs-Viewer wird plötzlich über den Task-Manager beendet.
- Das Netzwerk wird auf dem verwalteten Gerät oder auf der Verwaltungskonsole deaktiviert.

Unter bestimmten Umständen kann der Fernverwaltungsdienst bis zu eine Minute benötigen, um eine abnormale Beendigung der Sitzung festzustellen.

4.7 Erkennung unbefugter Benutzer

Durch die Funktion zur Erkennung unbefugter Benutzer wird das Risiko, dass das verwaltete Gerät von einem Hacker angegriffen wird, stark verringert. Wenn es dem Fernoperator nicht gelingt, sich innerhalb der angegebenen Anzahl von Versuchen (die Standardeinstellung ist 5 Versuche) beim verwalteten Gerät anzumelden, wird der Fernverwaltungsdienst blockiert und nimmt erst wieder eine Anforderung für eine Fernsitzung an, nachdem die Blockierung aufgehoben wurde. Der Administrator kann eine Blockierung des Fernverwaltungsdiensts entweder manuell oder automatisch aufheben.

4.7.1 Automatisches Aufheben der Blockierung des Fernverwaltungsdiensts

Die Blockierung des Fernverwaltungsdiensts wird automatisch nach Ablauf der in der Option *Annahme von Verbindungen automatisch starten nach [] Minuten beginnen* > in der Fernverwaltungsrichtlinie angegebenen Zeit aufgehoben. Der Standardwert beträgt 10 Minuten. Die Standardeinstellung kann in den Sicherheitseinstellungen der Fernverwaltungsrichtlinie geändert werden.

4.7.2 Manuelle Aufhebung der Blockierung des Fernverwaltungsdiensts

Sie können die Blockierung des Fernverwaltungsdiensts manuell über das verwaltete Gerät oder über das ZENworks-Kontrollzentrum aufheben.

Um die Blockierung des Fernverwaltungsdiensts über das ZENworks-Kontrollzentrum aufheben zu können, muss der Fernoperator über die Rechte „Blockierung des Fernverwaltungsdienstes aufheben“ für das verwaltete Gerät verfügen.

1. Klicken Sie im ZENworks-Kontrollzentrum auf *Geräte*.
2. Klicken Sie auf *Server* bzw. *Arbeitsstationen*, um die Liste der verwalteten Geräte anzuzeigen.
3. Wählen Sie das Gerät aus, dessen Blockierung aufgehoben werden soll.
4. Klicken Sie auf *Aktion* und klicken Sie dann auf *Fernverwaltungssperre aufheben*.
5. Klicken Sie auf *OK*.

So heben Sie die Blockierung des Fernverwaltungsdiensts über das verwaltete Gerät auf:

1. Doppelklicken Sie im Benachrichtigungsbereich des verwalteten Geräts auf das ZENworks-Symbol.
2. Wechseln Sie in der linken Kontrollleiste zu *Fernverwaltung* und klicken Sie dann auf *Sicherheit*.
3. Klicken Sie auf *Bei Blockade durch Erkennungsprogramm für unbefugte Benutzer Akzeptieren von Verbindungen aktivieren*.

4.8 Identifikation des Fernoperators

Wenn ein Fernoperator eine Fernsitzung über das ZENworks-Kontrollzentrum startet, wird automatisch ein Zertifikat erstellt, das dem verwalteten Gerät die Identifikation des Fernoperators erleichtert. Wenn der Fernoperator die Sitzung jedoch im eigenständigen Modus startet, wird das

Zertifikat nicht erstellt und der Fernoperator wird im Revisionsprotokoll sowie in den Dialogfeldern „Sichtbares Signal“ und „Benutzer um Erlaubnis fragen“ als *Ein unbekannter Benutzer* angegeben. Der Fernverwaltungsdienst ruft die ID des Fernoperators mithilfe des Zertifikats ab, das von der Verwaltungskonsole während des SSL-Handshake (Secure Socket Layer) bereitgestellt wird. Der SSL-Handshake erfolgt bei allen Authentifizierungstypen mit Ausnahme der VNC-Passwortauthentifizierung.

Der Fernverwaltungsdienst auf dem Gerät zeigt die Details des Fernoperators im Dialogfeld „Sichtbares Signal“ an, wenn die Option *Optisches Signal an Benutzer am verwalteten Gerät ausgeben* in der auf dem Gerät wirksamen Richtlinie aktiviert ist. Außerdem werden die Informationen des Fernoperators in den Fernverwaltungs-Revisionsprotokollen protokolliert.

4.9 Browserkonfiguration

Wenn Sie zum Starten von ZENworks-Kontrollzentrum auf Windows Vista-Geräten den Internet Explorer verwenden, müssen Sie den geschützten Modus in den Sicherheitseinstellungen des Browsers (*Extras* > *Internetoptionen* > *Sicherheit*) deaktivieren und den Browser neu starten.

4.10 Sitzungssicherheit

ZENworks Configuration Management verwendet Secure Socket Layer (SSL) zur Sicherung von Fernsitzungen. Fernsitzungen, die mithilfe der passwortbasierten VNC-Authentifizierung gestartet wurden, werden jedoch nicht gesichert. Der Authentifizierungsprozess erfolgt über einen sicheren Kanal, während der SSL-Handshake stattfindet, unabhängig davon, ob Sitzungsverschlüsselung in der Fernverwaltungsrichtlinie konfiguriert wurde oder nicht.

Nach Abschluss der Authentifizierung wechselt die Fernsitzung in einen unsicheren Modus, wenn die Option *Sitzungsverschlüsselung aktivieren* in der Fernverwaltungsrichtlinie deaktiviert ist und wenn die Option *Sitzungsverschlüsselung* vom Fernoperator während der Initiierung einer Fernsitzung auf dem verwalteten Gerät deaktiviert wird. Es wird jedoch empfohlen, die Sitzung in einem sicheren Modus fortzusetzen, da dadurch die Leistungsfähigkeit der Sitzung nicht nennenswert beeinträchtigt wird.

4.10.1 SSL-Handshake

Bei der Installation von ZENworks Adaptive Agent auf dem verwalteten Gerät generiert der Fernverwaltungsdienst ein selbstsigniertes Zertifikat mit einer Gültigkeitsdauer von 10 Jahren.

Wenn ein Fernoperator eine Fernsitzung auf dem verwalteten Gerät einleitet, wird er vom Fernverwaltungs-Viewer zur Überprüfung des Zertifikats des verwalteten Geräts aufgefordert. Das Zertifikat enthält Details wie den Namen des verwalteten Geräts, die ausstellende Zertifizierungsstelle, das Ablaufdatum des Zertifikats sowie den Fingerabdruck. Aus Sicherheitsgründen muss der Fernoperator die Berechtigungsnachweise des verwalteten Geräts überprüfen, indem er den Fingerabdruck des Zertifikats mit dem Fingerabdruck vergleicht, den er vom Benutzer des verwalteten Geräts mittels OOB- („Out-of-Band“-)Kommunikation erhalten hat. Anschließend kann der Fernoperator eine der folgenden Aktionen ausführen:

- **Das Zertifikat dauerhaft akzeptieren:** Wenn ein Benutzer, der sich bei der Verwaltungskonsole angemeldet hat, das Zertifikat dauerhaft akzeptiert, wird das Zertifikat in nachfolgenden Sitzungen nicht mehr angezeigt, die von auf dieser Konsole angemeldeten Benutzern eingeleitet werden.

- **Das Zertifikat vorübergehend akzeptieren:** Wenn ein Benutzer, der sich bei der Verwaltungskonsole angemeldet hat, das Zertifikat vorübergehend akzeptiert, wird das Zertifikat nur für die aktuelle Sitzung akzeptiert. Wenn der Benutzer das nächste Mal eine Verbindung zum verwalteten Gerät herstellt, wird er erneut zur Überprüfung des Zertifikats aufgefordert.
- **Das Zertifikat zurückweisen:** Wenn ein Benutzer, der sich bei der Verwaltungskonsole angemeldet hat, das Zertifikat zurückweist, wird die Fernsitzung beendet.

4.10.2 Zertifikaterneuerung

Das verwaltete Gerät erneuert ein selbstsigniertes Zertifikat unter folgenden Bedingungen:

- Der Name des verwalteten Geräts wurde geändert.
- Das Zertifikat ist vordatiert und noch nicht gültig.
- Das Zertifikat ist abgelaufen.
- Das Zertifikat läuft in Kürze ab.
- Das Zertifikat fehlt.

Das Zertifikat wird standardmäßig alle 10 Jahre erneuert.

5 Fehlersuche

In den folgenden Abschnitten werden Szenarios erläutert, die bei Verwendung der Fernverwaltungskomponente von Novell® ZENworks® 10 Configuration Management auftreten können.

- „Der Link „Fernverwaltungs-Viewer installieren“ bleibt auf einem Gerät unter Windows Vista, Windows 7, Windows Server 2008 oder Windows Server 2008 R2 aktiv, wenn auf dem Gerät Internet Explorer 7 installiert ist“ auf Seite 81
- „Möglicher Fehler bei der Installation des Fernverwaltungs-Viewers“ auf Seite 81
- „Der Fernverwaltungs-Viewer wird auf einem Gerät unter Windows Vista, Windows 7, Windows Server 2008 oder Windows Server 2008 R2 nicht gestartet“ auf Seite 81
- „Wenn Sie während einer Fernsteuerungssitzung im Fernverwaltungs-Viewer auf das Symbol „Strg+Alt+Entf“ klicken, werden im Fenster „Secure Attention Sequence“ (SAS-Fenster) unter Umständen keine Steuerelemente angezeigt.“ auf Seite 82
- „Bei Fernsteuerung oder Fernansicht des Geräts ist dessen Desktop möglicherweise nicht sichtbar“ auf Seite 82
- „Übertragung von Dateien via Fernzugriff in einen eingeschränkten Ordner auf einem Gerät unter Windows Vista, Windows 7, Windows Server 2008 oder Windows Server 2008 R2 nicht möglich“ auf Seite 82
- „Auf einem SUSE Linux Enterprise Server 11-Gerät kann über Mozilla Firefox keine Fernsitzung gestartet werden“ auf Seite 83
- „Der Link „Fernverwaltungs-Viewer aktualisieren“ wird nicht angezeigt, wenn Sie das ZENworks-Kontrollzentrum über Internet Explorer 8 starten“ auf Seite 83

Der Bildschirmschoner auf dem verwalteten Gerät kann nicht überschrieben werden.

Ursprung: ZENworks 10 Configuration Management; Fernverwaltung.

Erklärung: Wenn vor dem Start einer Fernsteuerungssitzung auf dem verwalteten Gerät ein passwortgeschützter Bildschirmschoner aktiviert ist, versucht der Fernverwaltungsdienst, den Bildschirmschoner zu überschreiben, damit der Fernoperator den Benutzerdesktop anzeigen kann. Der Fernoperator kann den Bildschirmschoner auch während der Fernsitzung überschreiben, indem er in der Symbolleiste des Fernverwaltungs-Viewers auf das Symbol *Bildschirmschoner überschreiben* klickt.

Mögliche Ursache: Wenn der Bildschirmschoner aktiviert wird, weil die Fernsitzung inaktiv ist.

Aktion: Klicken Sie in der Symbolleiste des Fernverwaltungs-Viewers auf das Symbol *Bildschirmschoner überschreiben*. Möglicherweise müssen Sie mehrfach auf das Symbol klicken, damit der Bildschirmschoner überschrieben wird.

Mögliche Ursache: Das Überschreiben der Bildschirmschonerfunktion wird auf Geräten unter Windows Vista, Windows 7, Windows Server 2008 und Windows Server 2008 R2 nicht unterstützt.

Aktion: Keine.

Mögliche Ursache: Der Bildschirmschoner kann unterbrochen werden, indem Mausbewegungen an das verwaltete Gerät gesendet werden.

Aktion: Wählen Sie im Fenster „Optionen des ZENworks-Fernverwaltungs-Viewers“ die Option *Mausbewegungsereignisse blockieren*, um zu verhindern, dass Mausbewegungen an das verwaltete Gerät gesendet werden.

Mögliche Ursache: Die GINA-Benutzerschnittstelle (Graphical Identification and Authentication) ist auf dem verwalteten Gerät aktiviert, weil der Bildschirmschoner auf dem verwalteten Gerät unterbrochen wurde.

Aktion: Melden Sie sich erneut beim verwalteten Gerät an.

Wenn Sie sich während einer Fernverwaltungssitzung bei einem Computer mit Windows 2000 Professional* ab- und wieder anmelden, wird der für den Computer festgelegte Bildschirmhintergrund möglicherweise nicht wiederhergestellt.

Ursprung: ZENworks 10 Configuration Management; Fernverwaltung.

Aktion: Keine.

Es kann keine Fernsitzung auf dem verwalteten Gerät gestartet werden, das mit einer sehr geringen Farbqualität ausgeführt wird.

Ursprung: ZENworks 10 Configuration Management; Fernverwaltung.

Erklärung: Auf einem verwalteten Gerät, das mit einer sehr geringen Farbtiefe ausgeführt wird (mit weniger als 8 Bit pro Pixel (bpp)), kann möglicherweise keine Fernsteuerungs-, Fernansichts- oder Ferndiagnosesitzung gestartet werden.

Aktion: Erhöhen Sie die Farbtiefe des Geräts auf 16 bpp oder höher, indem Sie das folgende Verfahren ausführen:

1. Klicken Sie mit der rechten Maustaste auf den Desktop.
2. Klicken Sie auf *Eigenschaften*.
3. Klicken Sie im Fenster „Eigenschaften von Anzeige“ auf *Einstellungen*.
4. Wählen Sie die entsprechende Farbtiefe aus und klicken Sie dann auf *OK*.

Der Fernverwaltungs-Viewer kann nicht gestartet werden.

Ursprung: ZENworks 10 Configuration Management; Fernverwaltung.

Mögliche Ursache: Der Fernverwaltungs-Viewer kann nicht gestartet werden, wenn die ausführbare Datei gelöscht oder umbenannt wurde.

Aktion: Installieren Sie den Fernverwaltungs-Viewer neu, indem Sie die aktuelle Version von `novell-zenworks-rm-viewer.msi` unter `https://`*`IP_Adresse_des_ZENworks-Servers`*`/zenworks-remote-management` herunterladen.

Abnormale Beendigung der Sitzung schlägt auf einem verwalteten Gerät unter Windows Vista, Windows 7, Windows Server 2008 oder Windows Server 2008 R2 unter Umständen fehl

Ursprung: ZENworks 10 Configuration Management; Fernverwaltung.

Erklärung: Wenn der Benutzer die Netzwerkverbindung während einer Fernsitzung auf einem verwalteten Gerät unter Windows Vista, Windows 7, Windows Server 2008 oder Windows Server 2008 R2 deaktiviert, kann ZENworks möglicherweise nicht erkennen, dass eine abnormale Beendigung erfolgt ist, und das Gerät wird nicht gesperrt bzw. der Benutzer auf dem verwalteten Gerät nicht abgemeldet.

Aktion: Keine.

Der Fernverwaltungs-Listener kann keine Fernsitzungsanforderungen vom verwalteten Gerät annehmen, wenn der Port, an den der Listener gebunden ist, in der Firewall der Verwaltungskonsole nicht geöffnet ist.

Ursprung: ZENworks 10 Configuration Management; Fernverwaltung.

Aktion: Öffnen Sie den Listener-Port in der Firewall der Verwaltungskonsole.

Während der Verwendung der Fernverwaltungskomponente werden Fehlermeldungen angezeigt.

Ursprung: ZENworks 10 Configuration Management; Fernverwaltung.

Aktion: Wenn während der Verwendung der Fernverwaltungskomponente Fehlermeldungen ausgegeben werden, senden Sie die folgenden Protokolldateien an den Novell Support (http://support.novell.com), damit dieser Ihnen bei der Behebung des Problems helfen kann:

- Die Dateien `WinVNCApp.log` und `WinVNC.log` (bei einem Gerät unter Windows Vista, Windows 7, Windows Server 2008 oder Windows Server 2008 R2)
- Die Datei `WinVNC.log` (bei anderen verwalteten Geräten)

So greifen Sie auf die Protokolldatei zu:

1. Öffnen Sie den Registrierungseditor.
2. Wechseln Sie in das Verzeichnis `HKLM\Software\Novell\ZCM\Remote Management\Agent`.
3. Erstellen Sie ein DWORD namens DebugMode und legen Sie als Wert 2 fest.
4. Erstellen Sie ein DWORD namens DebugLevel und legen Sie als Hexadezimalwert `a` fest (entspricht dem Dezimalwert 10).
5. Starten Sie den Fernverwaltungsdienst erneut.

Folgende Fernverwaltungs-Protokolldateien werden unter *ZENworks-Installationsverzeichnis*`\logs` erstellt:

- `WinVNC.log`
- `WinVNCApp.log`

Aktivieren des Debug-Protokolls zur Fernverwaltung auf dem Gerät, das das ZENworks-Kontrollzentrum startet

Ursprung: ZENworks 10 Configuration Management; Fernverwaltung.

Aktion: Informationen zum Aktivieren der Protokolle erhalten Sie im Artikel TID 3418069 in der Novell Support-Knowledgebase (http://support.novell.com/search/kb_index.jsp).

Installieren Sie eine neue Version des Mirror-Treibers.

Ursprung: ZENworks 10 Configuration Management; Fernverwaltung.

Mögliche Ursache: Bei der Installation von ZENworks Adaptive Agent auf einem verwalteten Gerät mit Windows 2003 64-Bit wird der Mirror-Treiber nicht auf dem Gerät installiert. Die Nachricht `Installieren Sie eine neuere Version des Mirage-Treibers` wird im ZENworks-Kontrollzentrum protokolliert.

Sie können Fernsitzungen auf dem Gerät durchführen, allerdings wird dadurch die Leistung beeinträchtigt.

Aktion: Ignorieren Sie diese Meldung.

Mögliche Ursache: Wenn Sie ein Gerät, das bereits mithilfe von Remote Desktop Connection (RDP) verbunden wurde, per Fernzugriff steuern, wird die Meldung `Installieren Sie eine neuere Version des Mirage-Treibers` im ZENworks-Kontrollzentrum protokolliert.

Sie können Fernsitzungen auf dem Gerät ausführen, die Ausführungsgeschwindigkeit ist jedoch reduziert.

Aktion: Ignorieren Sie diese Meldung.

Das verwaltete Gerät konnte kein Novell-Verschlüsselungsschema für die Sitzung initialisieren. Stellen Sie sicher, dass das verwaltete Gerät mit der UTC-Zeit dieses Systems synchronisiert ist. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support von Novell.

Ursprung: ZENworks 10 Configuration Management; Fernverwaltung.

Mögliche Ursache: Das verwaltete Gerät wurde aufgerüstet oder registriert und diese Informationen wurden nicht in der Registrierung des Geräts aktualisiert.

Aktion: Wenn das verwaltete Gerät aktualisiert oder registriert wurde, führen Sie die folgenden Aktionen aus:

1. Aktualisieren Sie den Domänennamen des neuen CA-Zertifikats in der Registrierung mit den neuen Details:

   Schlüssel: HKLM\Software\Novell\ZCM

   Wert: CASubject
2. Importieren Sie das CA-Zertifikat der neuen Zone in den vertrauenswürdigen Stammzertifikatspeicher.
3. Entfernen Sie das CA-Zertifikat der alten Zone aus dem vertrauenswürdigen Stammzertifikatspeicher.

Mögliche Ursache: Das verwaltete Gerät wurde in eine neue Verwaltungszone verschoben.

Aktion: Verwalten Sie das Gerät in der neuen Verwaltungszone.

Anwendungen wie Regedit können bei einem Start auf einem verwalteten Gerät mit einem 64-Bit-Betriebssystem über die Fernausführung nicht auf bestimmte Registrierungsschlüssel zugreifen.

Ursprung: ZENworks 10 Configuration Management; Fernverwaltung.

Mögliche Ursache: Anwendungen, die auf verwalteten 64-Bit-Geräten über „Fernausführung“ gestartet werden, werden in der WOW-Umgebung (Windows On Windows) ausgeführt.

Aktion: Starten Sie die Anwendungen über „Ferndiagnose“.

Die Option zum Ausblenden des Bildschirms kann während der Fernsteuerung eines Windows-Geräts möglicherweise nicht erfolgreich verwendet werden.

Ursprung: ZENworks 10 Configuration Management; Fernverwaltung.

Mögliche Ursache: Die Legacy-Treiber von Windows lassen keine Option zum Ausblenden des Bildschirms zu.

Aktion: Sie müssen den systemspezifischen Grafiktreiber installieren.

Beim Starten einer Fernverwaltungssitzung auf einem verwalteten Gerät mit Windows 2000 Professional bootet das Gerät neu

Ursprung: ZENworks 10 Configuration Management; Fernverwaltung.

Mögliche Ursache: Der Videotreiber ist nicht auf dem Gerät installiert.

Aktion: Sie müssen den systemspezifischen Videotreiber installieren.

Es werden mehrere Instanzen des Fernverwaltungs-Viewers auf einem Gerät mit dem Browser Internet Explorer 7 gestartet

Ursprung: ZENworks 10 Configuration Management; Fernverwaltung.

Mögliche Ursache: Wenn Sie einen Fernverwaltungsvorgang auf einem Gerät mit dem Browser Internet Explorer 7 starten, werden mehrere Instanzen des Viewers auf dem Gerät gestartet, wenn ein Download-Beschleuniger, wie beispielsweise FlashGet auf der Verwaltungskonsole installiert ist.

Aktion: Deaktivieren Sie vorübergehend die Add-ons für die Download-Beschleuniger:

1. Starten Sie den Browser Internet Explorer 7.
2. Klicken Sie auf *Extras* > *Add-Ons verwalten*.
3. Klicken Sie auf *Add-Ons aktivieren bzw. deaktivieren* und deaktivieren Sie dann das Add-on für den Download-Beschleuniger.
4. Starten Sie den Fernverwaltungsvorgang.

Aktion: Versuchen Sie, den Vorgang mit dem Browser Firefox durchzuführen.

Das Symbol „Strg-Alt-Entf“ ist bei der Fernsteuerung eines Geräts unter Windows Vista, Windows Server 2008 oder Windows Server 2008 R2 nicht verfügbar

Ursprung: ZENworks 10 Configuration Management; Fernverwaltung.

Erklärung: Wenn Sie einen Fernsteuerungsvorgang auf einem Gerät unter Windows Vista, Windows Server 2008 oder Windows Server 2008 R2 mit deaktivierter Benutzerkontensteuerung starten, ist das Symbol *Strg-Alt-Entf* abgeblendet.

Aktion: Aktivieren Sie die Benutzerkontensteuerung.

Der Standard-Sitzungsmodus ist im Fernverwaltungs-Snapin nicht ausgewählt

Ursprung: ZENworks 10 Configuration Management; Fernverwaltung.

Erklärung: Wenn Sie Internet Explorer verwenden, um das ZENworks-Kontrollzentrum zu öffnen und einen Fernverwaltungsvorgang an einem Gerät durchzuführen, wird der Standard-Sitzungsmodus nicht im Fernverwaltungs-Snapin ausgewählt. Wenn Sie jedoch keinen Sitzungsmodus auswählen, wird der Fernsteuerungsvorgang im standardmäßigen Zusammenarbeitsmodus gestartet und der Fernansichtsvorgang wird im standardmäßigen exklusiven Modus gestartet.

Aktion: Wählen Sie den Sitzungsmodus aus, um den Fernvorgang durchzuführen.

Der Link „Fernverwaltungs-Viewer installieren" bleibt auf einem Gerät unter Windows Vista, Windows 7, Windows Server 2008 oder Windows Server 2008 R2 aktiv, wenn auf dem Gerät Internet Explorer 7 installiert ist

Ursprung: ZENworks 10 Configuration Management; Fernverwaltung.

Erklärung: Auf einem Gerät unter Windows Vista, Windows 7, Windows Server 2008 oder Windows Server 2008 R2 mit Internet Explorer 7 wird der *Fernverwaltungs-Viewer* möglicherweise nicht installiert, wenn das ActiveX*-Steuerelement nicht aktiviert wurde.

Aktion: Gehen Sie wie folgt vor, um die Benutzerkontosteuerung (UAC) auf dem Vista-Gerät zu aktivieren:

1. Klicken Sie auf *Start* > *Einstellungen* > *Systemsteuerung* > *Benutzerkonten* > > *Benutzerkonten* > *Benutzerkontensteuerung ein- oder ausschalten*.
2. Wählen Sie die Option *Benutzerkontensteuerung verwenden, um zum Schutz des Computers beizutragen*.
3. Klicken Sie auf *OK*.

Aktion: Wenn Sie die Benutzerkontensteuerung auf dem Windows Vista-Gerät nicht aktivieren möchten, sollten Sie auf Windows Vista SP1 aufrüsten.

Möglicher Fehler bei der Installation des Fernverwaltungs-Viewers

Ursprung: ZENworks 10 Configuration Management; Fernverwaltung.

Erklärung: Die Installation des Fernverwaltungs-Viewers ist möglicherweise fehlerhaft. Dieser Fehler hat seine Ursache im MSI-Framework.

Aktion: Führen Sie einen der folgenden Schritte aus:

- Deinstallieren Sie den Fernverwaltungs-Viewer mithilfe der Systemsteuerungsoption „Software" und installieren Sie ihn neu
- Verwenden Sie das Microsoft Windows Dienstprogramm Installer Cleanup, um die Anwendung zu bereinigen und installieren Sie sie neu. Dieses Dienstprogramm kann von der Microsoft-Supportwebsite (http://support.microsoft.com/kb/290301) heruntergeladen werden

Der Fernverwaltungs-Viewer wird auf einem Gerät unter Windows Vista, Windows 7, Windows Server 2008 oder Windows Server 2008 R2 nicht gestartet

Ursprung: ZENworks 10 Configuration Management; Fernverwaltung.

Erklärung: Auf einem Gerät unter Windows Vista, Windows 7, Windows Server 2008 oder Windows Server 2008 R2 wird der Fernverwaltungs-Viewer nicht gestartet, auch wenn die Sicherheitsabfrage erfolgreich abgeschlossen wurde.

Aktion: Fügen Sie den Server, auf dem das ZENworks-Kontrollzentrum ausgeführt wird, zur Liste der vertrauenswürdigen Sites hinzu und versuchen Sie es erneut.

Wenn Sie während einer Fernsteuerungssitzung im Fernverwaltungs-Viewer auf das Symbol „Strg+Alt+Entf“ klicken, werden im Fenster „Secure Attention Sequence“ (SAS-Fenster) unter Umständen keine Steuerelemente angezeigt.

Ursprung: ZENworks 10 Configuration Management; Fernverwaltung.

Aktion: Klicken Sie im Fernverwaltungs-Viewer auf das Symbol *Strg+Alt+Entf* und drücken Sie anschließend die Esc-Taste, um das SAS-Fenster zu schließen. Klicken Sie danach im Fernverwaltungs-Viewer erneut auf das Symbol *Strg+Alt+Entf*.

Bei Fernsteuerung oder Fernansicht des Geräts ist dessen Desktop möglicherweise nicht sichtbar

Ursprung: ZENworks 10 Configuration Management; Fernverwaltung.

Erklärung: Bei Fernsteuerung oder Fernansicht eines Geräts, auf dem eine RDP-Sitzung durchgeführt wurde, wird anstelle des Desktops des Geräts möglicherweise nur ein leerer Bildschirm angezeigt.

Aktion: So zeigen Sie den Desktop des Geräts an:

1. Entsperren Sie den Desktop manuell.
2. Reinitiieren Sie eine RDP-Sitzung auf der Konsolensitzung des Geräts, indem Sie folgenden Befehl ausführen:

```
mstsc /console
```

Übertragung von Dateien via Fernzugriff in einen eingeschränkten Ordner auf einem Gerät unter Windows Vista, Windows 7, Windows Server 2008 oder Windows Server 2008 R2 nicht möglich

Ursprung: ZENworks 10 Configuration Management; Fernverwaltung.

Erklärung: Wenn Sie einen Dateiübertragungsvorgang starten, um Dateien via Fernzugriff in einen eingeschränkten Ordner auf einem Gerät unter Windows Vista, Windows 7, Windows Server 2008 oder Windows Server 2008 R2 zu übertragen, auf dem die Benutzerkontensteuerung (UAC) aktiviert ist, werden die Dateien nicht übertragen.

Aktion: Führen Sie zur Deaktivierung der Benutzerkontensteuerung auf einem Windows Vista-Gerät die folgenden Schritte aus:

1. Klicken Sie auf *Start* > *Einstellungen* > *Systemsteuerung* > *Benutzerkonten* > *Benutzerkonten* > *Benutzerkontensteuerung ein- oder ausschalten*.

2 Deaktivieren Sie die Option *Benutzerkontensteuerung verwenden, um zum Schutz des Computers beizutragen*.

3 Klicken Sie auf *OK*.

Aktion: Führen Sie zur Deaktivierung der Benutzerkontensteuerung auf einem Windows 7-Gerät die folgenden Schritte aus:

1 Klicken Sie auf *Start* > *Systemsteuerung* > *Benutzerkonten* > *Einstellungen der Benutzerkontensteuerung ändern*.

2 Verschieben Sie den Schieberegler auf die niedrigste Einstellung (*Nie benachrichtigen*).

3 Klicken Sie auf *OK*.

4 Starten Sie das Gerät neu.

Auf einem SUSE Linux Enterprise Server 11-Gerät kann über Mozilla Firefox keine Fernsitzung gestartet werden

Ursprung: ZENworks 10 Configuration Management; Fernverwaltung.

Erklärung: Das Fernverwaltungs-Plugin für Firefox wird im Verzeichnis `/usr/lib/firefox`, dem Standardinstallationsverzeichnis von Firefox, installiert. Wenn Sie Firefox auf dem SLES 11-Gerät in einem anderen Verzeichnis installiert haben, schlägt der Start einer Fernsitzung über Firefox auf diesem Gerät fehl.

Aktion: Kopieren Sie die Datei `nsZenworksPluginSample.so` aus dem Verzeichnis `/usr/lib/firefox/plugins` in das Verzeichnis mit den Firefox-Plugins.

Der Link „Fernverwaltungs-Viewer aktualisieren“ wird nicht angezeigt, wenn Sie das ZENworks-Kontrollzentrum über Internet Explorer 8 starten

Ursprung: ZENworks 10 Configuration Management; Fernverwaltung.

Erklärung: Wenn Sie das ZENworks-Kontrollzentrum bei einem Upgrade von ZENworks Configuration Management SP2 auf ZENworks Configuration Management SP3 über Internet Explorer 8 starten, wird der Link *Fernverwaltungs-Viewer aktualisieren* im ZENworks-Kontrollzentrum nicht angezeigt.

Aktion: Führen Sie die folgenden Schritte aus, um den Link *Fernverwaltungs-Viewer aktualisieren* anzuzeigen:

1 Starten Sie den Browser Internet Explorer 8.

2 Klicken Sie auf *Extras* > *Internetoptionen*, um das Dialogfeld „Internetoptionen“ anzuzeigen.

3 Klicken Sie auf die Registerkarte *Sicherheit*.

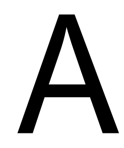
4 Klicken Sie auf die Option *Stufe anpassen*.

5 Stellen Sie sicher, dass folgende Einstellungen aktiviert sind:

- *ActiveX-Steuerelemente und Plugins ausführen*
- *ActiveX-Steuerelemente initialisieren und ausführen, die nicht sicher sind*

6 Starten Sie den Browser neu.

Detaillierte Informationen zur Kryptografie



Folgende Abschnitte enthalten die Details der verschiedenen Zertifikate, die während der Verwendung der Fernverwaltungskomponente von Novell® ZENworks® 10 Configuration Management generiert wurden.

- Abschnitt A.1, „Detaillierte Informationen zum Schlüsselpaar für verwaltete Geräte“, auf Seite 85
- Abschnitt A.2, „Detaillierte Informationen zum Schlüsselpaar für den Fernoperator“, auf Seite 85
- Abschnitt A.3, „Details zum Fernverwaltungsticket“, auf Seite 86
- Abschnitt A.4, „Details zur Sitzungsverschlüsselung“, auf Seite 86

A.1 Detaillierte Informationen zum Schlüsselpaar für verwaltete Geräte

Zertifikat erstellt von: Fernverwaltungsdienst

Zertifikat erstellt mit: OpenSSL v0.9.8e (Novell-Version)

Zertifikat signiert von: selbstsigniert

Zertifikat signiert mit: OpenSSL v0.9.8e (Novell-Version)

Zertifikat überprüft von: Fernverwaltungs-Viewer

Zertifikat überprüft mit: OpenSSL v0.9.8e (Novell-Version)

Verwendet von: Fernverwaltungsdienst

Verwendet für: Erstellung einer sicheren Sitzung mit dem Fernverwaltungs-Viewer

Privater Schlüsseltyp: RSA

Schlüsselstärke: 1024 Bit

Signaturalgorithmus: RSA-SHA256

Gültigkeit: 10 Jahre

A.2 Detaillierte Informationen zum Schlüsselpaar für den Fernoperator

Dieses Zertifikat ist nur bei Bereitstellung der internen Zertifizierungsstelle gültig

Zertifikat generiert von: ZENworks Server als Host des ZENworks-Kontrollzentrums

Zertifikat generiert mit: Bouncy Castle-Bibliothek (`bcprov-jdk15-134.jar`)

Zertifikat signiert von: ZENworks Server als Host des ZENworks-Kontrollzentrums

Zertifikat signiert mit: Bouncy Castle-Bibliothek (`bcprov-jdk15-134.jar`)

Zertifikat überprüft von: Fernverwaltungsdienst

Zertifikat überprüft mit: OpenSSL v0.9.8e (Novell-Version)

Verwendet von: Fernverwaltungs-Viewer und Fernverwaltungsdienst

Verwendet für: Herstellung einer sicheren Sitzung und Identifizierung des Fernoperators

Typ des privaten Schlüssels: RSA
Schlüsselstärke: 1024 Bit
Signaturalgorithmus: RSA-SHA1
Gültigkeit: 4 Tage

A.3 Details zum Fernverwaltungsticket

Dieses Zertifikat ist nur für die Authentifizierung der Rechte gültig

Ticket generiert von: ZENworks Server als Host des ZENworks-Kontrollzentrums
Ticket generiert mit: Bouncy Castle-Bibliothek (`bcprov-jdk15-134.jar`)
Zertifikat signiert von: ZENworks Server als Host des ZENworks-Kontrollzentrums
Ticket signiert mit: Bouncy Castle-Bibliothek (`bcprov-jdk15-134.jar`)
Zertifikat überprüft von: Fernverwaltungs-Web-Service (auf dem ZENworks-Server)
Zertifikat überprüft mit: Bouncy Castle-Bibliothek (`bcprov-jdk15-134.jar`)
Verwendet von: Fernverwaltungs-Viewer und Fernverwaltungs-Web-Service
Verwendet für: Authentifizieren des Fernoperators und Überprüfen der Rechte zur Durchführung eines Vorgangs
Signaturalgorithmus: RSA-SHA1
Gültigkeit: 2 Minuten

A.4 Details zur Sitzungsverschlüsselung

Sitzung erstellt zwischen: Fernverwaltungsdienst und Fernverwaltungs-Viewer
Verschlüsselungsprotokoll: SSL (TLSv1)
Sitzungs-Cipher: AES256-SHA
SSL-Authentifizierungsmodus: Gegenseitig/Server

B Optimale Verfahren

Die folgenden Abschnitte enthalten Empfehlungen zur Verwendung der Fernverwaltungskomponente von Novell® ZENworks® 10 Configuration Management.

B.1 Schließen des Fernverwaltungs-Listeners

Wenn ein Fernoperator den Fernverwaltungs-Listener startet, um Fernsitzungsanforderungen vom Benutzer des verwalteten Geräts zu überwachen, stellt ZENworks ein Ticket aus, das dem Fernoperator die Authentifizierung des verwalteten Geräts ermöglicht. Dieses Ticket ist zwei Tage lang gültig.

Der Fernverwaltungs-Listener wird auch nach Abmeldung des Fernoperators oder nach Beendigung des ZENworks-Kontrollzentrums weiter ausgeführt. Wenn das Ticket noch gültig ist, kann jeder andere Fernoperator den Listener verwenden, um Fernsitzungsanforderungen von Benutzern verwalteter Geräte zu überwachen. Aus Sicherheitsgründen müssen Sie den Fernverwaltungs-Listener beenden, bevor Sie sich abmelden oder den Browser schließen.

Klicken Sie zum Schließen des Fernverwaltungs-Listeners mit der rechten Maustaste auf das Symbol *ZENworks Remote Management-Listener* im Benachrichtigungsbereich und dann auf *Listening-Daemon schließen*.

B.2 Schließen von Anwendungen, die bei Fernausführungsvorgängen gestartet wurden

Standardmäßig wird das Fernverwaltungsmodul als Service mit Systemprivilegien auf dem verwalteten Gerät ausgeführt. Daher werden auch alle während der Fernausführungssitzung gestarteten Anwendungen mit Systemprivilegien ausgeführt. Aus Sicherheitsgründen wird dringend empfohlen, die Anwendungen nach Verwendung zu schließen.

B.3 Ermitteln des Fernoperators auf dem verwalteten Gerät

Wenn ein Fernoperator eine Fernsitzung auf einem verwalteten Gerät über das ZENworks-Kontrollzentrum startet, generiert ZENworks bei Verwendung einer internen CA automatisch ein Zertifikat, mit dessen Hilfe das verwaltete Gerät den Fernoperator ermitteln kann. Wird jedoch eine externe CA verwendet, muss der Fernoperator das Zertifikat, das mit der Zertifizierungsstelle verkettet ist und für die SSL-Client-Authentifizierung gilt, manuell angeben. Weitere Informationen zur Verwendung der externen CA erhalten Sie unter *Das folgende Schlüsselpaar zur Identifizierung verwenden* in Abschnitt 2.8, „Starten von Fernverwaltungsvorgängen“, auf Seite 36.

Wenn ein Fernoperator einen Fernvorgang auf einem verwalteten Gerät startet, ohne ein Zertifikat anzugeben, wird der Name des Fernoperators als *Ein unbekannter Benutzer* in den Überwachungsprotokollen und in den Dialogfeldern des optischen Signals und der Anforderung der Benutzerberechtigung aufgeführt. Stellen Sie sicher, dass der Fernoperator ein Zertifikat angeben muss. Deaktivieren Sie dazu in der Fernverwaltungsrichtline die Option *Verbindung zulassen, wenn Fernverwaltungskonsole über kein SSL-Zertifikat verfügt*.

B.4 Ausführen einer Fernsteuerungssitzung auf einem Gerät, das bereits über eine Remote-Desktop-Verbindung verbunden ist

Um ein Gerät, das bereits über eine Remote-Desktop-Verbindung (RDP) verbunden ist, fernzusteuern, muss eine der folgenden Bedingungen erfüllt sein:

- Die RDP-Sitzung wird auf dem verwalteten Gerät ausgeführt.
- Das verwaltete Gerät wurde manuell entsperrt, nachdem die RDP-Sitzung auf dem Gerät beendet wurde.

B.5 Ermitteln des Namens der Verwaltungskonsole

Wenn in der Fernverwaltungsrichtlinie die Option *DNS-Name des Viewers zu Beginn der Fernsitzung ermitteln* aktiviert ist, versucht das verwaltete Gerät, zu Beginn der Fernsitzung den Namen der Verwaltungskonsole zu ermitteln. Dies kann zu erheblichen Verzögerungen beim Starten der Fernsitzung führen, wenn im Netzwerk der Reverse-DNS-Lookup deaktiviert ist. Sie können die Verzögerung verhindern, indem Sie die Option *DNS-Name des Viewers zu Beginn der Fernsitzung ermitteln* in der Richtlinie deaktivieren.

B.6 Verwenden des Aero-Designs auf Geräten unter Windows Vista, Windows 7, Windows Server 2008 oder Windows Server 2008 R2

Zur Verbesserung der Leistung einer Fernsitzung verwendet die Fernverwaltung einen Mirror-Treiber, um die Änderungen am Bildschirm zu ermitteln. Wenn der Mirror-Treiber nicht mit dem Aero-Design kompatibel ist, wird beim Laden des Mirror-Treibers auf einem Gerät mit aktiviertem

Aero-Design automatisch zum Standard-Desktopdesign gewechselt. Dies kann sich auf die Benutzerfreundlichkeit auswirken. Deshalb wird empfohlen, das Aero-Design nicht auf fernverwalteten Geräten zu verwenden.

Wenn Sie das Aero-Design während der Fernsitzung des verwalteten Geräts beibehalten möchten, müssen Sie den Mirror-Treiber auf dem Gerät deaktivieren. Dazu müssen Sie die Einstellung *Optimierungstreiber aktivieren* auf dem Gerät deaktivieren. Weitere Informationen zur Einstellung „Optimierungstreiber aktivieren“ finden Sie im Abschnitt Konfigurieren der Fernverwaltungseinstellungen auf der Zonenebene.

Bei aktivem Aero-Design kann allerdings die Leistung der Fernsitzung auf dem verwalteten Gerät nachlassen.

B.7 Aktivieren der Schaltfläche „Software SAS“ (Strg-Alt-Entf) bei Fernsteuerung von Windows Vista- oder Windows Server 2008-Geräten

Um das Symbol (Strg-Alt-Entf) in der Symbolleiste des Fernverwaltungs-Viewers für die Fernsteuerung eines Windows Vista- oder Windows Server 2008-Geräts zu aktivieren, muss die Benutzerkontensteuerung auf dem verwalteten Gerät aktiviert sein.

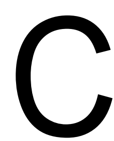
B.8 Installieren des Fernverwaltungsdienstes auf einem Windows XP-Gerät über RDP

Bei der Installation eines Fernverwaltungsdienstes auf einem verwalteten Gerät installiert ZENworks automatisch einen Mirror-Treiber namens DFMirage auf dem Gerät. Wenn Sie den Fernverwaltungsdienst auf einem Windows XP-Gerät über eine Remote-Desktop-Verbindung (RDP) installieren möchten, muss das auf der Microsoft Support-Website (http://support.microsoft.com/kb/952132) verfügbare Patch auf dem Gerät installiert sein.

B.9 Leistung der Fernverwaltung

Die Fernverwaltungsleistung während einer Fernsitzung über eine langsame oder eine schnelle Verbindung hängt auch vom Netzwerkverkehr ab. Informationen zu einer besseren Antwortzeit erhalten Sie unter Abschnitt 3.8, „Erhöhen der Fernsteuerungsleistung“, auf Seite 66.

Aktualisierungen für Dokumentationen



Dieser Abschnitt enthält Informationen zu Änderungen am Inhalt der Dokumentation, die in dieser *ZENworks Remote Management-Referenz* für Novell® ZENworks® 10 Configuration Management SP3 vorgenommen wurden. Sie haben hier die Möglichkeit, sich über die neuesten Aktualisierungen der Dokumentation zu informieren.

Die Dokumentationen für dieses Produkt stehen im Web im HTML-Format und als PDF-Datei zur Verfügung. Sowohl die HTML- als auch die PDF-Dokumentationen wurden im Hinblick auf die in diesem Abschnitt aufgeführten Änderungen auf den neuesten Stand gebracht.

Ob es sich bei der von Ihnen verwendeten PDF-Dokumentation um die neueste Ausgabe handelt, sehen Sie am Veröffentlichungsdatum auf der Titelseite des Dokuments.

An diesem Dokument wurden folgende Aktualisierungen vorgenommen:

- Abschnitt C.1, „30. März 2010: SP3 (10.3)“, auf Seite 91

C.1 30. März 2010: SP3 (10.3)

Die folgenden Abschnitte wurden aktualisiert:

Standort	Änderung
„Fernverwaltungs-Proxy“ auf Seite 12	Der Abschnitt wurde aktualisiert.
Abschnitt 1.3, „Zum Verständnis der Fernverwaltungsfunktionen“, auf Seite 14	Der Abschnitt wurde aktualisiert.
Abschnitt 2.5, „Konfigurieren des Fernverwaltungspassworts“, auf Seite 32	Der Abschnitt wurde aktualisiert.
Abschnitt 2.9, „Optionen zum Starten eines Fernverwaltungsvorgangs“, auf Seite 45	Abschnitt hinzugefügt.
Abschnitt 2.10, „Installieren eines Fernverwaltungs-Proxys“, auf Seite 50	Dem Abschnitt wurden Informationen zur Installation des Fernverwaltungs-Proxys unter Linux hinzugefügt.
Abschnitt 2.11, „Konfigurieren eines Fernverwaltungs-Proxys“, auf Seite 51	Abschnitt hinzugefügt.

Standort	Änderung
Abschnitt 3.7, „Reaktivieren eines entfernten Geräts“, auf Seite 64	Dem Abschnitt wurden Informationen zur Reaktivierung eines Geräts mit mehreren NICs hinzugefügt.
Abschnitt 3.6, „Verwalten einer Fernverwaltungs-Proxy-Sitzung“, auf Seite 64	Abschnitt hinzugefügt.
Kapitel 5, „Fehlersuche“, auf Seite 75	Die folgenden Szenarios wurden hinzugefügt: ◆ „Auf einem SUSE Linux Enterprise Server 11-Gerät kann über Mozilla Firefox keine Fernsitzung gestartet werden“ auf Seite 83 ◆ „Der Link „Fernverwaltungs-Viewer aktualisieren“ wird nicht angezeigt, wenn Sie das ZENworks-Kontrollzentrum über Internet Explorer 8 starten“ auf Seite 83
Kapitel 5, „Fehlersuche“, auf Seite 75	Das folgende Szenario wurde hinzugefügt: Die Fernübertragung von Dateien in eingeschränkte Ordner auf Windows Vista- oder Windows 7-Geräten ist nicht möglich
Abschnitt B.6, „Verwenden des Aero-Designs auf Geräten unter Windows Vista, Windows 7, Windows Server 2008 oder Windows Server 2008 R2“, auf Seite 88	Der Abschnitt wurde aktualisiert.